POL00423229

Contents

Page

Security

POL00423229

Contents

Page Page

Security

POL00423229

1 Introduction

This booklet provides all Post Office branch staff with the information required to adopt good basic security practices to keep staff safe from harm and Post Office® assets secure.

Although the majority of the information is based on contractual obligation, some instructions have been included as the result of best practice in Post Office branches around the country, which has proved simple to implement and of negligible cost.

Please note: This booklet is not intended to replace the instructions for security procedures written for and supplied to specific branch types, such as 'screen-less', 'Community', etc, nor does it supersede specific instructions relating to different types of security equipment that have been supplied to respective branches. Where applicable, this booklet is designed to be used as a supplement in tandem with other instructions you may have received.
For replacement instruction booklets relating to particular security equipment, you should contact the NBSC.

The practices included in this booklet apply to all branches unless otherwise stated. Headings have been added above the text in order to make it easier for you to determine which instructions apply to your type of branch. Please pay special attention, as in certain circumstances there are extra instructions for specific types of branch,'such as those without counter screens, ie, screen-less (see below) or those with particular types of security equipment.

Please remember: In order to ensure brevity of content, the term 'sub postmaster', when used throughout this booklet includes sub postmistress and nominee sub postmaster.

Adherence to correct security procedures

Adherence to mandatory security procedures is key to preventing unnecessary risks to the safety of staff and the security of cash, stock and Post Office® property, for if potential robbers see that stringent security procedures are in force at Post Office branches, this is more likely to deter them from carrying out criminal activity.

A failure to adhere rigidly to the security procedures in this manual may not in itself mean that a member of staff, an agent or his assistants is necessarily at fault, as managers, agents and staff are advised to consider the best course of action according to individual situations that occur, and a premium should always be placed on the safety and wellbeing of human life. However, in the same way, it may prove a significant consideration in a subsequent finding of fault, as failures to apply mandatory procedures will be viewed as a serious breach of contract, particularly if they are persistent.

To ensure continued compliance with mandatory security procedures designed to protect staff and assets:

- Ensure that you get to know and understand the security procedures that apply to your type of branch and ensure that they are carried out by everyone working in the branch
- Take the time to read this booklet regularly (at least every six months) to remind you of the procedures to follow and ensure that all staff are fully aware of their obligations to maintain security by following the correct procedures
- Always remember to take special care at vulnerable times such as opening and closing your branch, accepting and despatching Remittances, when balancing and when the branch is quiet.

Screen-less branches

While most of the procedures described in this booklet also apply to screen-less branches, extra care must be taken to safeguard cash and stock in a branch that does not have a screen.

Where additional information is supplied for screen-less branches, an appropriate heading has been added to the text, so that your branch can find the relevant instructions more easily.

Network Outreach services

Security instructions for the four new Network Outreach models have been included at the back of this booklet. Details are provided about the various branch types in operation, the equipment that is used, how cash and stock is transported and the business rules surrounding the carrying out of transactions.

POL00423229

Useful telephone numbers

Network Business Support Centre (NBSC)	GRO
Property and Facilities Helpdesk	GRO
RoMEC Security	GRO

2 Branch responsibilities

Sub postmasters and franchisees

A sub postmaster, nominee sub postmaster or franchisee is held strictly responsible for maintaining a standard of security sufficient to enable him to meet the obligations laid on him for the safe keeping of cash, stock and other Post Office property and documents, whether held in his care or that of his assistants, both during the day, and at night when the branch has closed.

Externally insured franchisees may also have additional requirements placed upon them by their insurance company.

A sub postmaster, nominee sub postmaster or franchisee is responsible for all losses caused through his own negligence, carelessness or error, and for losses of all kinds caused by his assistants. In addition to this, franchisees on some types of contract are responsible for all losses, irrespective of their cause.

A sub postmaster, nominee sub postmaster or franchisee must not without prior agreement of Post Office Ltd:

- move the branch to premises other than those in which it was situated at the time of appointment
- alter the accommodation for carrying out work on behalf of the Post Office from that which was agreed at the time of the appointment

Please note: If the branch premises include residential accommodation, the sub postmaster must inform the NBSC if he does not occupy this accommodation himself, if he ceases to do so, or if at any time it becomes vacant.

Crown Office Branch Managers

The Branch Manager is held strictly responsible for the safe keeping of cash, stock and other Post Office property and documents, whether held in his care or that of his assistants, both during the day, and at night when the branch has closed.

The Branch Manager must ensure that his staff are fully aware of mandatory security procedures and that they are correctly carried out.

The Branch Manager must also ensure that the Crown Office premises provide a secure working environment and that all security equipment is working correctly. Any faults discovered must be reported to the Property and Facilities Helpdesk on GRO immediately.

POL00423229

3 Opening and closing your branch

Opening and closing your branch are the times of day when you are most vulnerable to attack. Criminals may take advantage of any visible loopholes in security procedures to commit a crime. They may also break into premises and vehicles overnight and await the arrival of the staff the following morning.

Before entering your premises, or your vehicle, the following procedures must be followed:

Sub Office branches

Checking your branch and any vehicle you use

Non-residential premises

Please remember: The term 'non-residential branch' means a branch where the sub postmaster does not actually live on the premises.

- Check thoroughly any vehicle that you are about to use including the boot
- Vary your route to your branch on a regular basis and your time of arrival
- If you travel to work on foot, keep to well lit roads and vary the route of your walk as much as possible
- When you approach the branch, look out for strangers or people sitting in parked cars

Before you enter the premises:

- Check the exterior of your own and adjacent properties for signs of forced entry **where this is safe to do so**, paying special attention to any disturbance to brickwork (this must include the external perimeter of the property including the upper floors, external doors and windows)

Please note: At some high risk branches staff may expose themselves to greater risk by checking the rear of the premises. If this is the case at your branch, please contact the NBSC to arrange for a site assessment and special alternative procedures.

- Check the alarm box for signs of tampering (eg, wisps of foam protruding from the box)
- Look through the front window for any signs of disturbance.

If there is any sign of forced entry to your premises:

- Do not enter the premises
- Phone the Police on 999 and await their arrival
- Contact the NBSC to advise them of the situation.

Residential branches

Before you leave your residential accommodation:

- Check that you have a dialling tone when you lift the receiver of your phone (to ensure that your telephone lines have not been cut).

If there is no dialling tone on your phone:

- Do not enter the secure area of your branch
- Check outside the building for signs of any intruders
- If you are suspicious for any reason, use a mobile phone, a call box or a neighbour's phone to call the Police on 999
- Contact the NBSC to advise them of the situation.

Before you enter the secure area of your branch:

- Switch on the lighting (do not enter in the dark)

POL00423229

- Arrange, if possible, for a family member to act as a lookout and to keep the safe key until you have completed a search of the building.

If there is no internal route between the residential accommodation and the secure area of the branch:

- Check the outside of the building through a window or viewing panel before you leave the residential premises
- Then carry out security checks as for a non-residential branch (see above).

All types of Sub Office premises

When you have entered the Post Office premises:

- Make a thorough search of the premises to ensure that no obvious criminal activity has taken place.

Please remember: You must ensure that once you have carried out a thorough search, you can verify the results of the search to another party on the outside of the premises. It should be arranged that they will contact the Police should no message that the branch is safe be relayed to them within a specified timescale.

If more members of staff are expected for duty before the premises are opened to the public, and you have an electric door bolt fitted, this must not be used to admit staff. This is due to the possibility that a criminal could hide behind the counter and force the sub postmaster or a member of their staff to let further staff into the building, who would subsequently be trapped inside with the criminal(s).

- Always admit staff by unlocking and opening the front door in person.

Opening your branch for business and opening the main safe before you open

- Do not be tricked into opening the door before opening time by anyone seeking attention, whatever the pretext (criminals have been known to pose as Police officers (both plain clothes and uniform), postmen and members of the public requiring assistance after an accident).

When a time overlock is fitted to the safe, it must not be set to release more than 30 minutes before the official Post Office branch opening time. Earlier opening of the safe must be sanctioned in writing via the NBSC.

- Ensure that all exterior doors to the premises and, if applicable, any doors to residential premises are closed and locked before the safe is opened.

When you have opened the safe:

- Only hand out enough money for each member of staff to work for the first 1 to 1½ hours of business (working cash in the tills must be kept to an absolute minimum)
- Then close and lock the safe, withdraw the key and conceal it in the secure area (see subsection 5; page 16).

Before opening the door of the premises to the public:

- Ensure that all counter staff (except the one opening the door) are safely behind the counter screen (if there are members of staff permanently on the retail side of the business, one of these should open the front door)
- Check that the screen door and parcel hatch are closed and locked

Please remember: Where fitted, you must use the electric door bolt to open the front door to the public.

- Advise counter staff to watch the opening of the branch carefully so that they can set off a bandit alarm if an attempted attack or hostage-taking takes place.

Closing your branch (evenings and half-days)

You should always be extra vigilant at closing times especially regarding members of the public remaining in the branch when the outer door is closed.

- Organise a procedure for locking up and ensure that all staff understand what must be done.

If there are staff working in the retail side of the business at closing time, they must close and lock the door, and let the remaining customers out of the building. The electric door bolt must always be used to secure the door, where one is fitted.

POL00423229

Immediately your branch is closed:

- Lock all cash and stock in the safe as soon as cash has been checked for your final cash on hand declaration
- If one is fitted, set the time overlock to give maximum protection to the safe.

Please note: The time overlock must be set to release no more than 30 minutes before the Post Office branch opening time unless there is an operational need for earlier opening that has been sanctioned in writing via the NBSC. A copy of this written authority must be kept for audit purposes.

- If one is fitted, use the time delay lock compartment to secure bulk cash, leaving enough cash in the main safe for the first 1 to 1½ hours of business per working assistant the following morning.

If you do not have a time delay lock compartment, but two safes fitted with time locks are available, they must be used in the following way:

- Keep in one safe 1 to 1½ hours working cash and set the time overlock so that it releases no more than 30 minutes **before** the Post Office branch opening time
- Keep your bulk cash in the second safe and set the time overlock 30 minutes **before** the closure of your branch so that it will release 45 minutes **after** the Post Office branch opening time the following morning.
- Lock all safes and set all safe alarms
- Ensure that all windows and doors on the premises are closed and locked
- Ensure that any other Post Office alarms are set
- Before leaving your branch, look through the window to ensure that no strangers are lurking about
- If you are suspicious, do not go out (telephone the police using 999.

Leaving the branch

- Try to ensure that no-one is lurking outside your branch before you leave
- Leave through the front shop door whenever possible (if more than one person is present, one must act as a lookout while the other locks the door)
- Do not be tricked into going back into the branch, no matter what the reason and no matter what the request
- On the way home vary your route and always keep to well lit roads (if you feel you are being followed, drive or walk to a safe place, preferably the nearest Police Station)
- Never take items that appear in the 'Standards for secure storage' home with you (see 'Standards for secure storage of cash and value stock, etc' on page 20)
- Never attend your branch out of hours if requested to do so without first checking the validity of the caller (always dial 1471 to check a caller's number, never call back using the number given by the caller)
- Never return to your branch alone (ask the Police to meet you there and, if possible, get a family member or friend to accompany you
- If the Police are meeting you at your branch, always give them an estimated time of arrival.

Lunch times

When your branch (or the secure area of your branch) closes for lunch:

- Secure all cash and stock in the safe, even if you are remaining on the premises.
- Lock the safe, then withdraw the key
- Remove the safe key to another place of safety, away from the secure area.
- If an alarm (or time/electronic time overlock) is fitted to the safe, set the alarm and/or time overlock in order that the safe has maximum protection
- Lock the counter access door and ensure that the parcel hatch is closed.

POL00423229

If you are leaving the premises at lunchtime:

- Follow the evening locking up procedures (see 'Closing your branch (evenings and half-days)' on page 6)

When you return to the premises after lunch:

- Carry out the morning opening procedures (see 'Opening your branch for business and opening the main safe before you open' on page 6)

Balancing and counting cash at the close of business

Periods of balancing and counting cash are often vulnerable times for robbery. If you are balancing at night you are especially vulnerable if you are on your own in the branch.

Robberies often occur between 1715 and 1730 when criminals know that many branches have their safe doors open to count bulk cash. For this reason, you must only open the safe to count bulk cash once the branch has closed for business.

Always follow the procedures below to increase security:

- Always balance cash and stock immediately after the close of business
- Check bulk banknotes first so that you can secure them immediately in the safe
- Check your remaining cash and stock, then lock it all in the safe, withdraw the key and set the time locks, before completing the rest of your balance
- Be especially vigilant if you are balancing while the retail side of your business remains open
- Beware of phone calls or anyone calling at the door on the pretext they have left something behind

Crown Offices

First entry by cleaner

If your branch has a morning cleaner, and they are due to enter the premises first, the cleaner must obtain the branch keys and travel with an escort to your branch.

On arrival, the cleaner must check the perimeter of the premises for any visible signs of forced entry, while the escort stands a safe distance away, but within sight of the branch.

If there is evidence of forced entry, the cleaner or escort must notify the Police using 999, and then contact the ROMEC Alarm Receiving Centre on GRO to report the incident. They should remain a safe distance away from the premises until the Police arrive.

Please note: In these circumstances the cleaner and escort must not enter the premises before the Police arrive.

If there is no sign of forced entry, the cleaner must enter the premises through the designated official entrance door, lock the door behind them and make a thorough check of the entire premises. The escort must remain outside the premises, a short distance away until the search is completed.

When the search is completed, the cleaner must step outside the premises, lock the door and move away from the door to indicate that all is well. The escort must observe the cleaner's re-entry into the building before leaving.

Coded telephone call

At a specified time the cleaner must make a coded telephone call to a stipulated duty to indicate that all is well. A predetermined form of words must be used for the message. If there is any variation from this agreed form of words, the duty officer receiving the call must telephone the Police using 999 and contact the Branch Manager.

If the call is not received within five minutes of the scheduled time, the duty officer receiving the call must telephone your branch. If the answer is not satisfactory (in the agreed coded form), or there is no answer, they must telephone the Police using 999 and contact the Branch Manager.

POL00423229

Admittance of callers

Once inside the building, the cleaner must immediately secure the entrance door. After this, they must not open any outer door unless for reasons of personal safety, ie fire.

With the sole exception of their immediate supervisor, cleaners have no authority to give access to the branch to any other persons. This includes Post Office personnel (including postmen and audit inspectors); family members; friends; police etc. Nor must the cleaner admit the first branch staff to arrive, as they must carry out their own first entry procedures, including unlocking the door and checking the premises themselves.

Any persons seeking admittance to the branch must wait until branch staff are on duty to verify their authenticity.

First entry by Post Office Ltd staff (whether cleaner is on site or not)

First entry to the branch by Post Office Ltd staff must be made by two members of staff (designated as Keyholder A and Keyholder B).

Keyholder A must attend with the two door keys and the perimeter alarm key/code.

Keyholder B must have the siphon keys and safe key*.

*In branches where there are three people scheduled at the end of the day and the third individual takes the safe key, the safe key holder must not be scheduled for first entry and thus Keyholder B will only have the siphon keys. The safe keyholder must arrive after first entry procedures have been carried out.

Please note: Branch staff who perform a 'call-out' role, or who hold building access keys, must never act as Keyholder B.

Keyholders A and B must meet up at a pre-arranged point, where Keyholder B should hand the siphon keys to Keyholder A.

Keyholder B must remain outside until the all clear is given. This must be at a position a safe distance away from the branch, but within view, to act as look out (this will enable them to contact the Police if there is a problem).

Before they enter the branch, Keyholder A must check the exterior of the branch and adjacent premises for signs of forced entry. If signs of forced entry are evident, the branch must not be entered under any circumstances. One of the keyholders must phone the Police using 999 and then contact the NBSC on GRO selecting option 1 to report the incident.

When the external search of the branch has been completed, Keyholder A must enter the premises through the designated official entrance door and must lock the door behind them.

Please note: The designated official entrance door may not necessarily be the public access door. For operational reasons, it may be necessary for staff at some branches to enter through another door. However, there must be a valid reason why the designated official entrance door and the public access door are different doors, such as internally locking roller shutters being fitted. The public access door being further away from where staff park their cars is not a valid reason for its not being the designated official entrance door.

Keyholder A must carry out a full internal search of the whole branch.

This search **must** include:

- any disused areas of the premises if domestic facilities are located outside the Post Office branch secure area
- any areas at the back of the building that are not visible or accessible during the external search

The search **should not** include:

- separate occupied administration areas reached through siphon door systems
- any disused areas of the premises located through siphon door systems which are not normally entered at any time of the day, as long as domestic facilities are contained within the Post Office branch secure area

Once the internal search is completed, Keyholder A must return outside the premises, after locking the designated official entrance door behind them, to show that it is safe to enter.

If Keyholder B is distracted by someone speaking to them, Keyholder A inside the branch must remain there until the person distracting Keyholder B has moved off. Keyholders A and B must first make eye contact, if possible, before keyholder A exits the building.

POL00423229

Keyholder A must move away from the premises and physically go to Keyholder B.

Please note: A wave from inside the branch is not acceptable as a signal to the second keyholder that all is safe, as this could be carried out under threat from an intruder already on the premises.

Keyholders A and B must then both enter the branch, locking the official entrance door behind them.

If Keyholder B has the safe keys they must store them in the secure area out of visible site until it is time to open the main non-sub stock safe/s.

Admittance of regular staff

As further members of staff arrive, one member of staff must admit them through the designated official entrance door while another remains within the secure area adjacent to a bandit alarm and observes the procedure. A check must be made through the window, viewing panel or spy hole before the door is opened. The door chain (where fitted) may also be used. Each member of staff must be seen and identified before being admitted.

Please note: No other outer door except the designated official entrance must be used before the branch opens.

Whenever possible, it is recommended that staff members meet up away from the branch and enter as a group, thereby reducing the number of times the official entrance door has to be opened.

- Do not be tricked into opening the door before opening time by anyone seeking attention whatever the pretext (criminals have been known to pose as Police officers (both plain clothes and uniform), postmen and members of the public requiring assistance after an accident in order to gain unauthorised access to a branch).

Admittance of reserve staff

New or reserve staff due to attend your branch must carry an official identification document, a copy of which will have been previously e-mailed to the Branch Manager for comparison.

The identification document will show a unique serial number issued by the person sending the e-mail.

Coded telephone call by Post Office Ltd staff

When both first entry staff are safely inside the branch, keyholder B must make a coded security telephone call to a designated neighbouring Crown Office, at least 10 minutes before the branch is due to open, to indicate that all is well.

There must be an agreed form of words for call and answer. If you are the intended recipient of the call and you do not receive it within five minutes of the agreed time, you must telephone the Crown Office using the agreed form of words to check that all is well. If the reply is not the agreed form of words which you are expecting, or if there is no answer, you must inform the Police immediately using 999 and then contact the NBSC on GRO (selecting Option 1) to report the incident.

The form of words used for the security call should not in themselves cause suspicion and must be changed weekly in case a criminal becomes aware of the content.

Opening for business

The member of staff opening the public entrance door must not be in possession of the counter access door key (or siphon door key) when they open the door. The access door and parcel hatch must be closed and locked. Staff must be ready to sound the alarm in the event of an attack.

Before re-admitting the staff member into the secure area, a check must be made to ensure that no strangers are lingering by the access door, or attempting to gain access.

When a time overlock is fitted to the safe, it must not be set to release more than 30 minutes before the official Post Office branch opening time.

POL00423229

Closing the branch

At the close of business daily, the following security precautions must be taken:

The main safe/ strongroom must be locked and time overlocked at least 15 minutes before the branch is scheduled to close and remain locked until at least 15 minutes after the branch is scheduled to open to the public. This is a mandatory instruction, therefore any variation to this procedure must be agreed in writing via the NBSC, who should consult the local Security Manager.

If a personal attack alarm has been provided at the branch, the member of staff securing the outer door at the close of business must keep it on their person. After the main door of the premises is closed, it must only be opened to let customers out. No-one else must be admitted, on the pretext that they have forgotten something.

A check must be made that all counter drawers and pedestals are cleared and all valuable items are secured.

The time overlock on the counter stock safe(s) must be set by the safe keyholder and checked by keyholder A against a signature. The safe must be locked and the safe alarm set by the safe keyholder. When the safe keyholder is not keyholder B, they can now leave the branch.

Final exit

Exit by branch staff

If Crown Office counter staff are the final people on the premises, a minimum of two people must be present to carry out the final locking up arrangements. The safe keyholder must have left the premises before this takes place unless there are only two people available to complete the locking up.

A check of the public area must be made by Keyholder A to ensure that no one is remaining in the branch.

All windows and doors must be closed and locked. The keys in doors to areas of the branch that do not need to be kept secure (ie that have a low risk of break-in from outside) may be left in the keyholes. The keys to any siphon systems (other than the ones used during first entry procedures), external doors, stock rooms/ cupboards, ATM rooms, or other rooms that need to kept secure, must be locked in the key case, by keyholder A.

Please note: Cleaners must not have access to the key case. If cleaners require access to secure rooms, alternative secure storage to which the cleaners may have access (eg a pedestal drawer or lockable cleaners cupboard) will be required for these keys.

The alarm must be set for all areas protected by the alarm system by keyholder A (unless the cleaner is still on site).

Before leaving the premises, remaining staff must look through the window or viewing panel to check for any suspicious activity. If they see anything suspect, the door must not be opened until it is thought safe to do so.

If all is clear, the final alarm set button (where fitted) must be pressed before leaving the premises. If there is no cleaner on the premises, keyholder B must act as look-out while keyholder A secures the main door.

Please remember: Main exit doors must be fitted with at least one automatic deadlock but two are preferred, eliminating the use of a final exit key. The locks must be positioned at approximately one third and two-thirds the height of the door.

Exit by cleaner

If cleaners are left on the premises after counter staff leave, they must be instructed that:

- a check must be made to ensure that no persons are left on the premises
- nobody must be let into the premises on the pretext they have left something behind
- they should check that all perimeter doors and windows are closed and secured
- a check must be made that the alarm system is activated for all areas protected by the alarm system
- before leaving the premises they must look through the window or viewing panel to check for any suspicious activity (if they see anything suspect, they must wait in the branch until it is considered safe to leave or, if they feel under threat, they should telephone the Police using 999)
- the final exit alarm button must be pressed (where fitted)
- the final exit door must be securely closed and locked, using all available locks

POL00423229

Post Office Ltd insured franchise branches only

First entry by staff

Opening procedures must always be strictly applied, to prevent the likelihood of staff being held hostage as they arrive for work, particularly in the event of criminals having gained access to the premises overnight.

Each day must begin with a check of the Post Office operation secure area by staff entering first, even if non-counter staff are already in the building. A minimum of two people must carry out the procedure. The first person to enter the building must not be in possession of the Post Office safe key.

The two members of staff carrying out the first entry search must meet at an agreed meeting point away from the branch. One staff member must approach the designated official entrance door and, if possible, look through the windows to see if everything appears normal before entering. The other staff member must enter the branch, unset the perimeter alarm and make an internal search of the premises, while the first keeps watch outside, positioned a little distance away from the branch.

The staff member checking the premises must come out again, after locking the door and declare the branch safe.

Please note: A verbal okay from the secure area or a wave from inside the branch is not acceptable as a signal to the second member of staff that all is safe, as this could be carried out under threat from an intruder already on the premises.

If the person carrying out the search does not return in the agreed time, the staff member outside must not enter the branch. Instead they must telephone the Police and contact the NBSC to report the incident.

Once it is confirmed safe to do so, the two members of staff may enter the branch.

Each staff member can then be admitted to the Post Office area as they arrive. One person should open the door while another remains behind the screen with the access door locked, ready to activate the alarm should the need arise.

Please note: Whenever possible, it is recommended that other staff members meet up outside and enter as a group, after the initial entry has been made, thereby reducing the number of times the door has to be opened.

Each employee must be seen and identified through the window, viewing panel or spy-hole, as appropriate, before the door is opened to admit them on each occasion. Depending on the premises, the door chain should also be used. No outer door other than the designated official entrance must be used before the branch opens.

Please note: It is important that staff are aware that criminals may attempt to gain unauthorised entry by staging fake accidents, or posing as bogus policemen or postmen.

When reserve staff or Audit personnel visit, they must show identification so that their identity is confirmed before they are admitted to the premises. When in doubt as to the advisability of admitting a visitor, staff should contact the NBSC.

Coded telephone call

When the Post Office part of the premises opens before the retail side, a coded telephone call may be arranged between the branch and another suitable location, as an added security precaution.

A suitable form of words and reply should be agreed upon, together with the time that the call should be made, so that any variation to the arrangements suggests that a potential emergency may have occurred. If the intended recipient of the call does not receive it at the agreed time, they must call the Franchised branch, using the coded message. If the response is unsatisfactory or there is no reply, they should then call the Police using 999 and contact the NBSC immediately to report the incident.

A staff member should be nominated to make the call on a regular basis. For this reason, you must ensure that this particular arrangement is brought to the attention of all current and reserve (agency and temporary) staff and relief managers. It is recommended that a number of codes are used and rotated in case a criminal becomes aware of its existence.

POL00423229

Opening for business

- Do not be tricked into opening the door before your official opening time to anyone seeking attention whatever the pretext (criminals have been known to try to gain unauthorised access by posing as Police officers (both plain clothes and uniform), postmen and members of the public requiring assistance after an accident).

Where applicable, the access door and parcel hatch must be closed and locked before you open the public entrance door. The person opening the public entrance door must not be in possession of the counter access door key. Staff must be ready to sound the alarm in the event of an attack.

Before re-admitting the staff member opening the public door into the secure area, a check must be made to ensure that no strangers are lingering outside or attempting to gain access.

Cleaners

When cleaners are employed to clean the Post Office secure area, they must either carry out their duties during normal business hours or attend shortly before closing time to carry out evening cleaning.

Please note: It is not acceptable for the cleaner to be responsible for the initial opening of the Post Office branch.

Closing procedures

Final exit by staff

When the branch is closed (and it is not part of a larger retail outlet operating different hours of business), the main door must only be opened to let customers out and no-one else in on the pretext they have forgotten something. The staff member closing the main door must not be in possession of the key to the secure area.

The safe time overlocks must be set and checked by a second member of staff. Once the safe is closed and locked, the safe keyholder must leave the premises.

A minimum of two members of staff must be present to carry out the final locking-up arrangements. A check must be made of the public area to ensure that no-one is remaining on the premises. A check must also be made that all counter drawers and pedestals are cleared and all value items are secured.

All windows and internal doors must be closed and locked and the keys to the doors secured in the key case. The burglar alarm must be set for all areas protected by the alarm system.

Before leaving the premises, the two members of staff locking up must look through the window or viewing panel to check that it is safe to leave the premises. If they see anything suspicious, the door must not be opened until it is thought safe to do so. Then the final exit alarm button must be pressed (if the branch has one).

One person should act as look-out while the other secures the main door.

Final exit by cleaner

If cleaners are left on the premises after counter staff leave, they must be instructed that:

- a check must be made to ensure that no persons are left on the premises
- nobody must be let into the premises on the pretext they have left something behind
- they should check that all perimeter doors and windows are closed and secured
- a check must be made that the alarm system is activated for all areas protected by the alarm system
- before leaving the premises they must look through the window or viewing panel to check for any suspicious activity (if they see anything suspect, they must wait in the branch until it is considered safe to leave or, if they feel under threat, they should telephone the Police using 999 and contact the NBSC to report the incident)
- the final exit alarm button must be pressed (where fitted)
- the final exit door must be securely closed and locked, using all available locks

If a cleaner is working alone, they must take adequate precautions before leaving the branch. They must look out the window or viewing panel to check for any suspicious activity. If they are suspicious of anything outside, they should wait in the branch until they consider it is safe to leave or telephone the local Police station.

Cleaners must be left with appropriate contact details which would allow them to deal with any issues that arise when setting the alarm system (eg, system failure).

POL00423229

4 Protection of the counter area and premises

You must always adopt the following general rules for protection of the Post Office area of your premises:

- Ensure that all parts of the property associated with the Post Office are kept as secure as possible
- Whenever possible, set all alarms in any unoccupied areas
- Ensure that the windows and doors in any attached residential premises are kept as secure as possible if the area is left unattended (in particular, doors from any residential accommodation into the secure area must be kept closed and locked with the key withdrawn unless this is part of a fire escape route, in which case the key should be left in the lock).

In addition, the instructions relating to specific equipment protecting the secure part of the premises, relating to each type of branch are as follows:

4.1 Counter access doors

All branches

Security siphon doors

If your branch has security siphon doors:

- Please ensure that all staff are aware of the function of the siphon doors and the protection they afford
- Check regularly that they are functioning as follows:

- the interlocking must operate so that only one door can open at a time
- locks and component parts must be fully secured with no screws missing or loose
- the buzzer indicating that the door is open must be functioning and all controls must be clearly marked

- Only admit one person at a time into the secure area through the siphon doors.

After someone has entered through the first (furthest) door:

- Always check through the viewing panel before you open the second door in case a second party has gained unauthorised access when the first door was opened.

All doors into the Post Office secure area

All doors into the secure area must be kept closed and locked, and the key withdrawn at all times, unless this forms part of a fire escape route, in which case the key should be left in the lock. Keys to the secure area must not be left on hooks, counter tops or shelves etc or within drawers or tills which can be accessed by criminals or members of the public.

When staff members leave the Post Office secure area, the keys to any counter access doors must remain with staff left within the Post Office secure area. Re-entry to the Post Office secure area is then controlled by staff within this area. The only exception to this is when no staff remain within the Post Office secure area. In this instance the keys to the counter access door must remain on the sub postmaster's or other responsible staff member's person.

Admittance of visitors

All visitors must be formally identified before you admit them to the secure area of your branch.

- Always keep a written record (in a booklet or on loose paper) of all visitors, including Post Office Ltd staff, who require access to any part of the premises other than the public area (including behind the counter in screen-less branches)
- Ensure that each visitor signs this record upon arrival, and records the date and time of their visit and their departure
- Keep all records of arrivals and departures of visitors for a minimum of two years
- Ensure that no visitor is allowed unwitnessed access to cash and stock.

POL00423229

Post Office Ltd staff

Post Office Ltd staff must plan in advance with the Branch Manager, the sub postmaster or the franchisee any visit that they need to make to a branch. The only exceptions to this are visits from senior managers as part of their visiting programme, security managers, and audit inspectors.

The visitor must give their name, the purpose of the visit and an estimated time of arrival. On arrival at the branch visitors must produce an identity card so that their identity can be verified.

If further confirmation of identification of any individual is required or there is doubt as to whether any visitor should be admitted to your branch:

- Please telephone the NBSC on GRO who will confirm the identity of any cardholder by asking one or two security questions.

Audit inspectors

All audit inspectors have a Post Office Ltd identity card, so that you can verify their identity.

On no account must the safe be unlocked or access given to cash, stock or Cash Account documents until an inspector's identity has been confirmed.

Sometimes at a branch with extended opening hours an audit check may start before 8 am. In this circumstance the audit inspector will present the sub postmaster/Branch Manager, etc with a letter on headed notepaper which gives details of the Post Office being audited and the telephone number of the appropriate Audit Manager who can verify the audit.

Post Office contractors

Visits by contractors carrying out repairs or maintenance within Post Office branches will be arranged in advance and the contractors will carry identity cards.

Other visitors

Some government; local authority and utility company personnel have a statutory right of access to business premises. Others do not. A full check of these visitors' credentials must be made before access is given.

If you are in doubt as to the validity of any visitor:

- Please telephone the NBSC.

If the visit takes place during Post Office business hours:

- Do not open the safe under any circumstances if the visitors are within the secure area.

If there is an operational need to open the safe:

- Ask the visitors politely to leave the secure area until the safe has been secured.

Please remember: You must not allow any visitor to your branch access to Post Office funds.

Visitors requesting longer access to the secure area must be asked to make an appointment to return out of Post Office business hours, when all cash and stock have been secured.

Public access

Members of the public must only be allowed access to defined areas and never allowed access to secure areas of the branch or behind screen-less counter positions.

Crown Offices only

The maintenance of counter access doors in Crown Offices is the responsibility of the Property and Facilities team.

- Report any damage or wear and tear to the Property and Facilities Helpdesk immediately.

POL00423229

Screen-less branches

When the public has access to the premises, a member of staff within the secure area must control access from the open plan area into the secure area. Keys to the secure area must always be held in the secure area.

4.2 Anti-bandit screens (and parcel hatches)

All branches

An anti-bandit screen is the glass screen at the counter that divides the Post Office secure area from the public side of the premises. The purpose of the screen, which is part of the counter fixtures and fittings in most branches, is to deter personal attacks and to prevent value items from being snatched.

The anti-bandit screen supports should extend to the ceiling and the gap between the screen and the ceiling should be filled. There must be no gap at the side of the screen and the counter or at the side of the door.

On older (Mk 1) types of anti-bandit screen the four corner bolts on the parcel hatch must be checked and tightened regularly, as this will reduce the problem of broken sash springs and increase resistance in an attack.

Please remember: A poorly fitted or incomplete screen, or a failure to properly seal off the rest of the counter, can compromise the security that the screen affords.

The anti-bandit screen must also be kept clear of posters, so that there is always an unrestricted view of the shop area.

The parcel hatch is the secure access point in the anti-bandit screen which may be opened to receive parcels and large letter items from customers directly across the counter.

For details of screens specific to Sub Post Office branches and Crown Offices, see para 17.4, page 54 and page 55.

5 Safeguarding keys

Sub Office branches only

It is the sub postmasters' responsibility to keep all keys associated with their Post Office branch secure at all times.

All doors into the Post Office counter area must be kept closed and locked, and the key must be withdrawn at all times, unless the door is on a fire escape route, when the key should be left in the lock.

The keys to the access door and safe must always be kept on separate key rings.

When staff members leave the Post Office counter area, the keys to any counter access doors must be left with staff within the Post Office counter area, unless no staff remain there, when the keys to the counter access door must be kept by the sub postmaster or another responsible staff member.

During the day keys to the secure area must never be left on hooks, counter tops or shelves, etc. or within drawers or tills that can be accessed by criminals or members of the public. Where a coin container is installed, the key to the container can be locked in the safe overnight or kept on the same ring as the safe key.

All working keys must be removed from the premises after the close of business and kept at home in a secure place, except for (where fitted) the 26L alarm 'B' key and alarm interface keys. These must be locked in the main safe at all times, together with the reverse set of 'B' and interface keys.

You must have an operational and duplicate set of keys, and they should be changed over at six monthly intervals to ensure that keys and locks wear evenly. Duplicate keys, if not issued to a member of the family or another member of staff, must be kept in a secure place in case of an emergency

If you have a third copy of the safe key, it must also be kept in a secure place, but in a separate place to the second key.

If you have trouble remembering the security arrangements for each key, you should refer to the table shown below:

POL00423229

Type of key	Working Set		Reserve Set	
	Number Of Keys	Where this must be kept	Number Of Keys	Where this must be kept
Safe	1	On its own concealed in secure area	1 or 2 dependent on type of safe	At home
Post Office alarm C	1	Both in sub postmaster's possession	1	At home
Counter access door	1		1	
Post Office alarm B	1	Both in Post Office safe	1	Both in Post Office safe unless time overlock is fitted*
Interface	1		1	

*. If a time overlock is fitted inside the door of the main safe the reserve 'B' key and interface key may then be retained in a secure place such as a non time-locked Post Office safe, private safe or lockable cupboard.

Post Office Ltd insured franchise branches only

Keys to the premises

It is essential that all keys to your branch are kept safe, and given the level of security which they warrant. The ultimate responsibility for key security lies with the manager. Keys must not be left hanging from locks where they are accessible to criminals.

A full and proper record of **all** keys issued and transferred to members of staff must be maintained at all times.

At no time should any one member of staff (including the Branch Manager) be in possession of keys for both the public entrance and the secure counter access (or siphon) doors while they are on the public side of the counter, except in the case of first entry procedure (see 'First entry by staff' on page 12). Staff re-entering the secure area must always be admitted by another employee.

Safe and strongroom keys

Safe and strongroom doors must be kept locked whenever immediate access is not required. The keys must be kept by the person to whom they were issued at all times. When transferred, they must be signed for and a record kept of the person who has responsibility for their safekeeping.

Duplicate keys must be kept in a sealed envelope against a code and retained securely off-site.

The operational and duplicate set of keys must be changed over at six monthly intervals to ensure that keys and locks wear evenly.

Internal door keys

Internal door keys must be kept in a metal lockable key case. The keys must be identified by a numerical code only. A key code index must be maintained and kept in separate secure storage.

The key case must always be kept closed and locked when not in use, even during normal hours of business.

All duplicate keys must be individually labelled with a discreet code, placed in a sealed envelope and kept away from the branch under secure conditions.

POL00423229

Crown Offices only

Keys to the premises

It is essential that all keys to your branch are kept safe, and given the level of security which they warrant, as described below. The ultimate responsibility for key security lies with the Branch Manager. Keys must not be left hanging from locks where they are accessible to criminals.

The keys for the designated official entrance door and the counter access (or siphon) doors must be divided into two bunches (Bunch A must consist of two door keys and the alarm/key code and Bunch B must be the siphon keys and safe key*).

*In branches where there are three people scheduled at the end of the day and the third individual takes the safe key, the safe key holder must not be scheduled for first entry and thus Keyholder B will only have the siphon keys. The safe keyholder must arrive after first entry procedures have been carried out.

During branch opening hours the keys on Bunches A and B must be kept secure by the Branch Manager or their deputy for as long as is practical.

Overnight these bunches of keys must be kept by separate persons. This is so that no single person can gain access to the premises. The Branch Manager or their deputy must maintain a daily record, of which member of staff takes responsibility for Bunch A and B overnight, and the related locking up procedures. The appropriate members of staff must sign for the keys each day, so that an audit trail of key responsibility can be maintained.

Once the Branch Manager or their deputy arrives at the branch each day Bunch A and B keys must be handed back to them as soon as possible. The manager of their deputy should sign the daily record of key responsibilities to indicate that they have once again taken responsibility for the keys.

Please note: At no time should any one member of staff (including the Branch Manager) be in possession of keys for both the public entrance and the secure counter access (or siphon) doors while they are on the public side of the counter, except in the case of first entry procedure (see 'First entry by Post Office Ltd staff (whether cleaner is on site or not)' on page 9). Staff re-entering the secure area must always be admitted by another employee.

Safe and strongroom keys

Safe and strongroom doors must be kept locked whenever immediate access is not required. The keys must be kept by the person to whom they were issued at all times. When transferred, they must be signed for and a record kept of the person who has responsibility for their safekeeping.

Duplicate keys must be kept in a sealed envelope against a code in a neighbouring Crown Office. The details of the location details must be kept by the Branch Manager.

The operational and duplicate set of keys must be changed over at six monthly intervals to ensure that keys and locks wear evenly.

Internal door keys

Internal door keys must be kept in a metal lockable key case. The keys must be identified by a numerical code only. A key code index must be maintained and kept in separate secure storage.

The key case must always be kept closed and locked when not in use, even during normal hours of business.

All duplicate keys must be individually labelled with a discreet code, placed in a sealed envelope and kept secure in a neighbouring Crown Office safe (unless agreed local arrangements differ).

POL00423229

6 Security of cash and value stock

All branches

Vigilance is required at all times to safeguard the security of cash, stock and Post Office property and protect it from robbery and burglary.

Anything of a suspicious nature that occurs in your branch must be reported immediately to the Police and the NBSC with a description of any person(s) involved.

Please note: In the following instructions the term 'safe' or 'official safe' means 'any safe used to secure Post Office cash and stock, etc' and the term 'main safe' means 'the official safe fitted with most items of security equipment (eg, time overlock (electronic or mechanical), time delay lock, time delay compartment, alarm).

Working cash and stock, etc

Cash and stock levels at the counter must always be kept to an operational minimum.

Cash must be restricted to whatever is required for immediate operational needs and must never exceed the amount that each working assistant or counter clerk would reasonably require for 1 to 1 ½ hours work at any one time. Excess cash accepted from customers in transactions must always be transferred to the main official safe as soon as possible.

Banknotes, stock, Motor Vehicle Licences, etc, must not be left on the counter top, or in full view of the public on any other work surface or by any open parcel hatch, where they can be hooked out or snatched through any gaps in the anti-bandit screen, or where they would encourage an attack on the screen. In the same way, banknotes, stock, etc, must not be kept in boxes on the counter top. Ideally, counter drawers should be used to secure these items, but if boxes are used, they must be kept below counter level.

Datestamps must also be kept secure at all times. They must be kept away from any gaps in the anti-bandit screen large enough for them to pass through, and they must not be left where they can be grabbed when the parcel hatch is opened.

Cash and value stock kept in safes

You must never keep excess cash (more cash than you need to keep the counter operating) in counter stocks and you must always transfer excess cash to your official safe as soon as it is operationally possible to do so.

For details of alternative secure storage where cash and value stock may be secured during periods when you are waiting for the time lock on the main safe to open, or the collection of a Remittance, see subsection 17, page 42, 'Secure storage other than the main safe'.

Opening the safe

You must not open the official safe(s), main or otherwise, more than 30 minutes before your official Post Office branch opening time (even if you operate a private business alongside), unless there is an operational need for earlier opening that has been sanctioned in writing via the NBSC. A copy of this written authority must be kept for audit purposes.

Please note: In the case of Crown Offices, instructions about opening the safe can be found below the heading 'Opening for business' on page 10.

If you are unable to time lock your safe due to mechanical breakdown, you must inform the NBSC.

Official safes of all types and strongrooms must be kept locked when not in immediate use. Safe doors must never be left open just for a few minutes' convenience. Even when you are serving a customer who requires cash or stock that is secured in an official safe, you must close and lock the safe door before you return to the customer with their requirements.

Whenever possible, rooms and enclosures containing official safes and strongrooms must be kept locked when the safes are in use, particularly if there is access to the counter.

Protecting the safe with security equipment

Maximum use must be made of any security equipment provided (eg time overlocks, time delay locks, time delay lock compartments, security cameras, smoke packs and alarms).

POL00423229

If you are unsure how to use any item of security equipment with which you have been provided:

- Please contact the NBSC for advice.

If you have a private business attached to your branch:

Takings from your private business may be kept in an official Post Office safe overnight providing that:

- private cash is kept in a box with a secure lid, completely separate from official Post Office funds and is clearly marked as such
- it still means that there is room for all official Post Office cash and stock to be stored securely in the safe
- time locks (if fitted) on the safe are set to reflect official Post Office business hours, **not** the private business hours if these are different.

Standards for secure storage of cash and value stock, etc

Your safe must provide secure storage and satisfactory robbery protection for all of the cash and value stock for which you have responsibility. It must be kept locked, with the keys removed, when not in immediate use. The keys must be concealed from public view.

Please note: Safe keys must not be left on hooks, counter tops, or shelves, or within drawers or tills, that can be accessed by criminals or members of the public.

During business hours bulk cash and stock (and any other valuable items that are unlikely to be required immediately) must at all times be secured in your main official safe and full use made of time overlocks, time delay locks and time delay lock compartments, where fitted. Full details of stock items that must be secured in this way are shown in the first table below (items that may be given a reduced level of security are shown in the tables that follow). Sufficient cash and stock for 1½ hours working per person should be kept on the counter and this should be replenished from the main safe as required.

Outside of business hours all items of cash and stock must, ideally, be kept in a Post Office Ltd safe or its equivalent, providing satisfactory burglary protection.

If you do not have adequate secure storage space for all cash and stock items in a main safe, you must use the available space to the best advantage, according to the comparative value of individual items to be stored (see tables below). You should advise the NBSC of any problems that you have with secure storage space in your branch, so that provision can be made for additional storage as soon as possible.

If a safe provided by a contractor other than Post Office Ltd is used, a comparable level of security must be given to the items in the table below as far as the secure storage in your branch will permit.

Items that must be stored in a main official safe

Please note: The items in the table below are given in priority order of importance for secure storage, with the items on the left, top to bottom, having precedence over those on the right.

Banknotes (English, Scottish, Northern Ireland, and euros)	Travellers' Cheques
Foreign currency	Commemorative coins
Motor Vehicle Licence discs	Activated National Lottery Scratchcards (Instants)
Post Office saving stamps	Pre-authenticated lottery cheques
Postage (including Stamp Books and rolls)	Open Girocheques
Philatelic items containing Special Stamps	Post Office Phonecards
Travel permits (including Centro) and bus tickets	Mobile Phone Prepay and Ringtone Vouchers
Rod Fishing Licences	Datestamps

POL00423229

Postal Orders	Travel Insurance documents
Home Care stamps	Gift Vouchers
Electricity Meter Tokens	Documents relating to transactions which missed your collection cut-off

Please note: Banknotes, value stock, Motor Vehicle Licences and datestamps must not be left on the counter top or in open view on any other work surface where they can be hooked out of the secure area, snatched through gaps in the anti-bandit screen, or grabbed through an open parcel hatch, nor should they be left exposed so that they invite any attack upon the counter screen from the public side.

Boxes on counter tops must not be used to serve banknotes and stock from. Ideally, under-counter drawers should be used. Where boxes are used they must be kept below counter level.

Items that may be stored in any type of safe

Unactivated National Lottery Scratchcards (Instants)

Items that may be stored in a lockable coin or security cabinet

Coin **Please note:** If you have limited space for securing items, ensure that highest denominations of coin are locked away first. If necessary, lower denominations can be left out of secure storage.	
Meals on Wheels vouchers	

Items that may be stored in a lockable cupboard or drawer

Vault Cards (for the Post Office card account)	Paid DWP Girocheques
National Lottery printer rolls	Postage Labels
Datestamp type	Cheques
Game Licences (Scottish and Northern Ireland branches only)	'Refer to drawer' cheques
Philatelic items (other than those locked in the main official safe)	Garden Refuse Tickets
Stamped Stationery	Laundry tickets/tokens

POL00423229

Absence from workstation

Extreme care must be taken if you leave your counter position to obtain a form, or any other item. Items such as datestamps, stamp books, Motor Vehicle Licences and Postal Orders must not be left in a position where they can be snatched.

If you are in a branch that does not close for lunch, you must secure all items of value in your counter pedestal or drawer when you vacate your counter position for a lunch break (or any other break during the day). Drawers must be closed and locked if possible and the keys kept secure by the relevant member of staff.

Transfer of cash and stock during business hours

Any staff transferring cash and stock to and from the secure area and the retail area of a branch (eg, staff on a 'late start' or 'early finish', or those removing Lottery cash in order to pay prizes) must be extra vigilant in checking that there is no suspicious activity occurring in the branch when they transfer the cash and stock.

Another member of staff must act as observer, and be in a position to activate the alarm, if necessary, until the transfer is complete.

Please note: These instructions apply equally to the transfer of cash and stock to and from the open plan area of a screen-less branch.

Sleight of hand confidence tricks

There are certain transactions that confidence tricksters use in order to carry out sleight of hand fraud activity. When successful, they manage to obtain several hundred pounds at the expense of branches, who suffer the associated losses.

The fraudsters target transactions involving large amounts of Sterling, and in particular Bureau de Change transactions, but fundamentally their tactics remain the same. The customer will ask to change a large amount of banknotes, £10 notes into £20 notes or Sterling into foreign currency.

After having obtained the banknotes that they have requested, the customer will then make an excuse to change their mind so that they no longer have to continue with the transaction and demand a refund of the original notes. The branch neglects to count the money returned by the customer, assuming that they have given back the correct amount. However, on further inspection after the customer has left, it is discovered that a large amount of the returned money is missing.

Please remember: Branches are responsible for losses of this type, so please remain vigilant in these circumstances. You must always count money received or returned by customers to ensure that the amount is correct before you complete a transaction.

A similar confidence trick to beware of is when a customer asks to feel a bundle of notes as they are intending to send cash in the post and they need to understand how big an envelope to use. Counter staff have then given the customer cash, following which the fraudster runs out of the branch without returning it. Please be careful not to become a victim of this trick.

Screen-less branches

While the procedures relating to security of cash and stock in this subsection relate equally to screen-less branches, extra care must always be taken to safeguard cash and stock in a working environment that does not have a counter screen.

POL00423229

Cash limits

Branches that use teller cash dispensers must not keep more than £350 at each counter position (including coin).

For screenless branches that use cash funding units, the drawer or the flip top till of the open plan desk must only keep £600 in cash at the counter position at any one time. All excess coin not kept in the coin hopper should be secured in a lockable drawer.

Please note: Any other available cash exceeding £600 must be dispensed into the cash funding unit or drop safe (if fitted).

- You must carry out all transactions over £600 (both inpayments and outpayments) through a dedicated secure position.

The management of remaining cash will be dictated by the security procedures associated to the type of cash management system installed in the branch (eg, a teller cash dispenser or roller cash unit).

Cash funding units or teller cash dispensers must be loaded and unloaded of cash outside of business hours with the branch doors locked.

Please remember: The safety of all staff, Sub postmasters and customers must come first and the Personal Attack alarm must only be activated when it is safe to do so.

Securing cash and stock

You must always adhere to the following guidelines for the security of cash and stock items:

Cash, stock and documents must be secured in the pedestal drawer or a flip top till at all times and must not be left on top of the screen-less counter in view of customers
Confidential documentation must not be left in a position where it can be read by customers
The datestamp must be secured with a suitable retaining wire or stored under a counter shelf or in a lockable drawer when not being used
The stamp folio must be secured to a retaining chain or stored under a counter shelf or in a lockable drawer when not being used
Motor Vehicle Licences must be retained in the dispenser provided
All cash and stock holdings must be kept to a minimum level. Replenishing of cash and stock at intervals is preferable to overstocking
Immediately after close of business all value cash and stock must be withdrawn from the screen-less serving positions and secured in safe or strongroom accommodation

Vacation of a screen-less serving position

Cash, stock items, datestamps, stamp folios and Motor Vehicle Licences must never be left unattended. They must always be locked away when you vacate a serving position.

If a desktop mounted Motor Vehicle Licence unit is provided, it must be removed from the desk and stored in suitable secure accommodation in the secure area, when a serving position is vacated.

POL00423229

7 Serving disabled customers who cannot gain access to the premises

In order to comply with the Disability Discrimination Act (DDA), Post Office Ltd, and its sub postmasters and franchisees all have a responsibility to give disabled customers the same access to products and services as able-bodied customers.

However, problems may arise at some branches in the provision of access for disabled customers who cannot physically pass through the public entrance door, particularly older premises with steps or narrow doorways.

Sub Office and Post Office Ltd insured franchise branches

Under the Disability Discrimination Act (DDA), it is the responsibility of the sub postmaster or franchisee to ensure that their business premises are capable of entry by disabled customers, or that provision is made for them to access products and services.

In exceptional circumstances it is permissible to serve disabled customers outside of the branch. You must take no more than £600 cash and stock combined, outside of the branch at any one time in order to serve disabled customers. It must be understood that the sub postmasters' or franchisees' responsibility for the cash/stock ends when it is handed over to the customer.

If you are a sub postmaster in a single manned branch, and you need to serve a disabled customer outside of your secure area, you must close and lock the safe, and the counter access door, when you leave the secure area.

Crown Offices only

Most Crown Offices have access for disabled customers.

If disabled access is not possible at your branch and this causes problems for you when serving disabled people, you must raise the issue with Property Holdings.

8 Security of mail (including Mails Integrity)

8.1 Mails Integrity

All branches

From 1 January 2006 a new Postcomm licence condition (Mails Integrity) came into force. This requires all postal operators to minimise the risks to mail of loss, damage, theft and interference. under the terms of this licence it is essential that all Post Office Ltd employees and sub postmasters and their assistants/representatives fully understand, and are fully trained in and compliant with the 'Mails Integrity' code of practice.

To ensure that you comply with the code of practice:

- Never delay items of mail or open them without reasonable excuse
- Ensure that you do everything you can to prevent mail being stolen, lost, damaged or tampered with.

In addition, **all** individuals in sub Post Office branches, franchise Post Office branches or other agency branches, including sub postmasters, franchisees and other agents, officers in charge, managers, staff, substitute staff, Post Office Partners and their staff, must complete the 'Regulatory Compliance Workbook' as part of their induction and ongoing training.

Sub postmasters who contract with Post Office Ltd to offer 'Outreach services' must ensure the requirements of the code are met at all Outreach locations, particularly when items of mail are transported between an outreach site and the supporting 'Core' branch.

POL00423229

It is essential that every effort is taken by sub postmasters of 'Core' branches and their representatives to minimise the exposure of postal items to the risk of loss, theft, damage or interference. Particular attention must be paid to ensure that:

- mail, including pouches and bags, is not left unattended or in an unauthorised or an unsafe place
- Special Delivery (where available) and other priority mail items are afforded appropriate protection and are not left unattended (they must be kept in a locked drawer or cupboard until despatched
- when transported between 'Outreach' and 'Core' sites, mail items are secured in the boot of the vehicle (if the vehicle is left unattended, the doors and windows of the vehicle must be locked, and Special delivery items must not be left unattended in the vehicle)

Please note: It is the responsibility of the sub postmaster to register all staff and/or representatives with Human resources in Salford to ensure that recruitment identification checks are completed.

Failure to ensure that satisfactory steps have been taken to protect mail items may lead to disciplinary action.

Any questions relating to mails integrity procedures should be addressed to your field Change Adviser or your Business Development Manager.

Receiving mail at the counter

One reason why mail may fail to arrive or arrive in a damaged condition is that it is not in a suitable state to be accepted in the first place.

This means that, when you accept mail from customers at the counter, you must check while the customer is still present that:

- the mail item is properly addressed
- the mail item is securely and appropriately packaged
- a sender's address has been recorded on the item

Full details of the conditions of acceptance for mail items can be found in the appropriate section of the Operations Manual; Inland mail services or International mail services booklet.

Handling of mail

All mail items must be treated in the same manner (ie, handled carefully), whether or not they have been marked 'fragile'.

Not opening or delaying mail

In the normal course of mail acceptance there is no reasonable excuse for delaying or opening postal items.

For details of what to do if you believe that you may have come into contact with a suspect package, see para 24.2; page 92.

Correct acceptance of Priority Service items

When you accept Priority Service mail items you must always follow the correct procedures:

- Always keep the items locked in secure accommodation in the secure area of your branch, until they are collected
- Always ensure that mail items are handed directly to the Royal Mail Collection Officer at the time of despatch and that items are properly recorded and signed for

Screen-less branches

Enhanced mail service items must be kept in a lockable drawer with the key secured by staff or immediately transferred to a secure area or position.

Keeping all mail items you have accepted in a safe place

Mail must only be accepted during official Post Office hours of business.

POL00423229

Whenever you accept an item of mail at the counter, you must keep it:

- out of the reach of members of the public
- safe from the risk of theft or loss
- secure from damage

Please remember: Whenever it is not in use, you must keep the parcel hatch closed and locked.

At some branches postmen may deliver mail pouches for collection later in the day. The safeguards listed above must also be applied in this instance.

Whenever a customer leaves unattended mail on the public side of your branch:

- Immediately collect the mail and store it in your branch secure area.
- If you are concerned about your safety whilst doing this, or are suspicious of the persons leaving the mail on the public side, wait until the person has left your branch.

Please note: You must not advise or allow customers, under any circumstances, to leave mail unattended at vacant serving positions, parcel hatch positions, parcel transfer units or any other unsecured position.

Screen-less, part screen-less and Rising screen branches

You must keep mail items in a secure container in your controlled area behind the counter serving positions until they are collected by the Royal Mail Collection Officer.

Please note: If you do not have a controlled area behind the counter, provision must be made to provide a suitable container that secures the mail from public or unauthorised access. If you need advice regarding this, telephone the NBSC on GRO selecting option 3. They will arrange a suitable solution in consultation with the appropriate departments within Post Office Ltd and Security.

After close of business:

- Ensure that any mail items that have not been collected are secured in a controlled area to prevent public and unauthorised access.

8.2 Reporting incidents relating to mail items

All branches

Any incidents involving the following must always be reported to the NBSC on GRO option 3:

- theft of mail
- loss of mail items
- interference with mail items
- damage to mail items

Please remember: This applies whether there is a suspicion or accusation of dishonesty, or whether the incident is due to negligence or error.

8.3 Siting of scales

All branches

Letter and parcel scales must be sited on the public side of the counter whenever possible and securely screwed down. This will minimise the amount of times you need to take larger items into the secure area in order to weigh them.

If space cannot easily be found to position your scales, you should consider attaching a small shelf to the front of the counter.

POL00423229

8.4 Acceptance/transfer of mail at doors, parcel hatches and siphons

Branches with parcel hatches and/or siphons

Acceptance of mail through parcel hatch siphons, single operation parcel hatches, either in doors or built into the counter and under counter parcel transfer units must be controlled at all times.

The doors on the customer side of parcel hatch siphons, single operation parcel hatches, either in doors or built into the counter and under counter parcel transfer units must be fully closed at all times when not in immediate use.

Parcels must always be accepted through the appropriate parcel acceptance unit.

If your branch has a parcel hatch:

- Beware of tricks such as dummy parcels designed to get you to open the hatch
- Do not open the hatch unless you consider it safe to do so
- Do not leave it open longer than necessary
- Do not leave items of mail in the parcel hatch, items must be cleared immediately upon receipt and secured
- Never use it as an extra general serving position
- Always test your parcel hatch weekly to see that it is operating safely
- Report any faults that you find as soon as possible.

Whenever you accept a parcel or a larger size packet:

- Only open the parcel hatch as far as it takes to accept the parcel
- Never move away from the open parcel hatch to place the parcel on the secure side of the counter
- Do not move away from or, turn your back on the open parcel hatch, even for a moment (criminals often use opportunities like this to gain unauthorised access to a branch through an open hatch)
- Close the hatch immediately the item has been accepted.

Please remember: Mail must not be left on the public side of the counter under any other circumstances.

Branches without parcel hatches

If your branch does not have a parcel hatch, you must make provision for accepting and securing large items of mail to prevent customer and unauthorised access. However, this must not increase any other security risk nor prevent compliance to the security standards shown in this booklet.

Part screen-less, part fortress branches

Mail can either be accepted at the Fortress or Screen-less positions.

Fortress branches

Mail items must be accepted at the counter positions or through a parcel hatch, and stored in the secure area.

If you have any mail containers outside of the secure area that are accessible to the public, you must remove them to prevent unauthorised access.

8.5 Transfer of mail between the secure area and the public side

All branches

If you leave the secure area of your branch:

- Ensure that you always leave the keys to any counter access doors with the staff left within the secure area.

POL00423229

Re-entry to the secure area must then be controlled by the staff within the secure area. The only exception to this would be where no staff remain within the secure area. In this instance the keys to the counter access door must remain on your person.

Keys to the secure area must not be left on hooks, counter tops or shelves etc. or within drawers or tills that can be accessed by potential attackers or members of the public.

- Keep all doors to the secure area closed and locked. Keep the keys in a metal lockable key case at all times.

8.6 Collection of mail

Mail collections must only be made during official Post Office hours of business. The only exception to this instruction is when premises are open for business outside of these hours, and mail can be kept safe outside the Post Office secure area.

All items of mail and Royal Mail pouches must be secured in either the Post Office secure area or in a controlled area to prevent public or unauthorised access until they are collected by the Royal Mail Collection Officer.

A Collection Officer **must not** be allowed to make a collection unless they have first produced the correct card authorizing them to collect from your branch.

Please note: All casual staff, (which are generally employed at pressure periods i.e. Christmas), must carry appropriate identification and this must be produced before they can be allowed to collect any mail.

If you are suspicious of a Collection Officer:

- Telephone the local Royal Mail Collection unit to check identification before handing over your mail.

Whenever the Royal Mail Collection Officer calls to collect your mail:

- Transfer mail items to the Royal Mail Collection Officer through the parcel acceptance unit or the security siphon doors when they are provided
- Do not admit Royal Mail Collection Officers into the secure area, unless they are designated to work behind the counter as part of their duty (in this case they should sign in and out and their identity should be checked before they enter the secure area)
- Keep the counter access door closed and locked. Keep the keys in a metal lockable key case at collection times.

Royal Mail staff assigned to a branch

Some branches that accept large amounts of mail may have dedicated Royal Mail staff allocated to the branch for part, or all of the day. If this applies to your branch, you must:

- Establish a regular contact point in Royal Mail so that you can obtain the information you need relating to cover
- Obtain from Royal Mail the times of attendance for their staff and an assurance that security procedures will be carried out correctly
- Ensure that you have been advised of details of all Royal Mail staff from your relevant parent office, prior to your allowing access to the branch
- Request evidence of identity on a daily basis, even from familiar Royal Mail staff
- Ensure that Royal Mail staff are not allowed to operate doors into the secure area (this must be left under the control of the branch staff)
- Ensure that you adopt a procedure for regular signing on for Royal Mail staff (the information captured must be name in block capitals, signature, badge number, time of arrival and time of departure)

Please note: All branch staff must be advised of the procedures for signing on of Royal Mail staff so that records can be maintained on a regular basis.

- Prepare instructions for Royal Mail staff to detail the procedures that must be followed in your branch
- Ensure that all mail collections follow a standard procedure (ie, mail is transferred through a siphon system, parcel hatch or pen)
- Review procedures regularly and carry out snap checks to ensure compliance with existing procedures
- Restrict access to the serving area as far as possible.

POL00423229

9 Security of items relating to other transactions

9.1 Acceptance of Alliance & Leicester business deposits and change giving services

All Alliance & Leicester business deposit payments must be accepted at the counter. You must not allow depositors entry into the secure area of your branch.

You should make full use of siphons/ transfer units, where installed, to avoid direct contact between staff and depositors when carrying out cash transfers (including bulk coin deposits and change giving services).

9.2 Securing documents

All documents relating to transactions carried out on behalf of clients must be kept secure at all times. Any applications accepted after the last collection and which cannot be despatched must be locked in a safe overnight. Under no circumstances must they be left unsecured.

Please remember: If any documents are lost, stolen or tampered with, the integrity of Post Office Ltd could be compromised with our clients and the possibility of future contracts jeopardised.

Photocard Driving Licences and Identity and Passport Service (IPS) applications

In particular, you should be very careful in securing any Photocard Driving Licence documents or documents supporting Identity and Passport Service (IPS) applications (eg, Birth or Marriage Certificates, old passports) that are kept in your branch, as these are very valuable to criminals and terrorists.

Applications for the DVLA Premium Service and the IPS Check & Send Service which are accepted before your last mail collection must be despatched at the end of the day.

Applications accepted after your last mail collection must be locked in your safe overnight. You must not under any circumstances leave them unsecured.

Please remember: It is absolutely vital that procedures to ensure the security and integrity of the applications handled on behalf of the DVLA and the IPS are complied with.

Sub Office branches

National Lottery transactions

Cash

Lottery cash in the till in the retail area of your branch must be kept to a minimum, currently no more than £250.

Amounts in excess of £250 must be transferred to the secure area during business hours as soon as it is safe and operationally possible to do so, or must be secured in a drop safe or a cash deposit box at the private (retail) till.

At the close of normal Post Office hours of business remaining Lottery cash must be transferred to and locked away in the secure area of your branch.

Scratchcards

Activated Scratchcards should be collected from the secure area of your branch by retail staff and placed in the appropriate dispensers whenever fresh supplies are needed, in order to maximise sales.

Please note: The security of Scratchcards on the retail side is the responsibility of the sub postmaster and they should be kept to the minimum number which will cover expected sales. Post Office Ltd will accept liability for no more than the equivalent of one day's sales in respect of theft, and will pursue excessive losses when negligence is proved to have occurred.

The dispensers should be secured to the retail counter.

POL00423229

You should maintain an audit trail of the funds which are transferred from the Post Office side of your business to the retail side, and the excess cash that is transferred from the retail side to the Post Office side. For information on how to do this, see the National Lottery booklet; Scratchcards; General information; para 8.11, Security of cash and transfer of funds.

At the close of business, Scratchcards must be removed from the dispenser and locked up overnight. They must not be left in the dispenser overnight.

'Out of hours' transactions

As the main official safe must be time locked and the alarm set at the close of normal Post Office hours of business, suitable arrangements must be made for securing Lottery cash if you transact National Lottery business outside of these hours, or for valuable items for any other type of transaction carried out 'out of hours'. In these circumstances National Lottery cash may be secured in a second official safe or a suitable private safe.

Cash for Lottery and any other 'out of hours' business in the till in the retail area of your branch must be kept to a minimum, currently no more than £250.

For information on which prize payments may be made in the retail area of your branch and when you should advise customers to return when the secure area of your branch is open, see National Lottery booklet; On-line games; para 6.2; Paying prizes.

Crown Offices

National Lottery transactions

Branch Managers should use the following guidelines to form a set of procedures for the maintenance of security relating to National Lottery transactions which are suitable for their individual branches.

The following points need to be taken into consideration when a suitable procedure is formulated:

- the amount of cash generated by National Lottery transactions
- the position of the lottery terminal
- the security equipment available

Please remember: All staff working at the lottery position must be fully trained on appropriate security procedures. They must be made aware of the importance of minimising cash holdings and reporting suspicious circumstances to the Branch Manager.

Cash held at the lottery till must not exceed £250. Full use must be made of counter caches, cash safes or other cash deposit containers, where provided, for lottery cash. Cash kept in these must not exceed £1500.

The keys to the cash safe or container must always be kept by the Branch Manager in the secure area. Under no circumstances should they be kept at the lottery position.

In order to maintain an acceptable level of cash on the public side of the counter, it may be necessary to transfer surplus money to the counter during the day, or transfer extra funds to the public side from time to time from the lottery till or cash safe. The volume or pattern of business will dictate how often this is required. As far as possible, the cash should not be transferred at set times in case a regular pattern of activity becomes obvious to anyone who may be intending to carry out a robbery.

Care must always be taken when staff leave and return to the secure area. They should check that nobody is loitering near the lottery position. If they are doubtful about any activity on the public side of the counter, they should not transfer cash or stock until it appears safe to do so. Whenever possible, the member of staff carrying the cash should be escorted by another member of staff with a personal attack alarm.

Please note: Under no circumstances should cash be counted in public view outside of the secure area and on the public side.

All lottery cash must be transferred to the secure area at the close of business and secured in the main safe.

Scratchcards

Scratchcard dispensers should be secured to the area surrounding the retail till.

POL00423229

The maximum number of Scratchcards displayed must never exceed one day's worth of sales. For further information on the security of Scratchcards and the amount that should be placed on display, see the National Lottery booklet; Scratchcards; para 8.10, Loss or theft of scratchcards.

At the close of business Scratchcards must always be secured within the main safe or strongroom and not left on display.

'Out of hours' transactions

If an 'out of hours' service is provided for the Lottery (or any other transaction), bulk Lottery cash and stock, etc, must be secured in the main safe in the normal way at the close of normal hours of business. The safe must be time locked, the alarm set, and all datestamps locked away.

Cash taken for 'out of hours' Lottery (and other) transactions must be secured in a lockable deposit box and this must be kept in the secure area at all times when your branch closes. It must be kept to a minimum, currently no more than £250.

Please note: Any branch wishing to provide an 'out of hours' service must first contact the NBSC.

Screen-less branches

Vacation of serving positions

Cash, stock, datestamps, stamp folios and Motor Vehicle Licence discs must never be left unattended and must be locked away when vacating a serving position.

Where a desktop mounted Motor Vehicle Licence unit is provided, it must be removed from the desk and stored in suitable accommodation in the secure area.

10 Security procedures for Automatic Teller Cash Machines

ATMs have been installed at many branches in the Post Office network over a period of years, and a number of contracts are now in place with different financial institutions, although the current ATM programme involves the installation of Bank of Ireland ATMs at approximately 4000 branches.

This subsection explains the security procedures relating to the operation of Automatic Teller Cash Machines (ATMs) at Post Office branches. You should follow the instructions applicable to your ATM provider and the type of equipment installed at your branch. Some instructions apply to all ATMs.

POL00423229

10.1 Bank of Ireland ATMs: Internal ATM Procash 1500 and External ATM Procash 2050

The Internal ATM Procash 1500 and the External ATM Procash 2050 are illustrated below:

Security instructions

You must always comply with the following security procedures for this make of ATM:

In the case of Internal ATMs, the maximum daily cash limit for an internal ATM is £30,000; the overnight limit must not exceed £20,000; In the case of External ATMs, the maximum cash that can normally be deposited is £140,000, though some branches have been authorised to fund the machine in excess of this figure. Authority to hold in excess of the normal amount must always be in writing.
Your ATM must be protected by a fully monitored alarm system.
Cash awaiting transfer to your ATM must always remain secured within your time-delayed main safe.
Other than when you are filling your ATM with cash, the ATM keys must be kept at all times in your time-delayed main safe. This means that the keys have time over-locking for overnight protection.
For the purposes of initial training, £600 of cash may be entered in the ATM while your branch is open for business.*
You should not remove the remaining cash from your ATM overnight, unless you do not have arrangements for a Police response to your alarm system.
Access to the ATM must only be permitted out of business hours, or when the premises are closed and no members of the public are on site* (this applies to external ATMs when the ATM backs on to the public area of the branch).

POL00423229

The time delay on the ATM safe must not be started while members of the public are in your branch.*
While you are replenishing the cash in your ATM, all doors to your branch must be locked and secured to prevent access from the exterior of the premises.*
It is recommended that two persons refill the ATM with cash: one person should remain vigilant adjacent to a personal attack alarm button and one should refill the ATM.
You must ensure that any view that the public may have of the ATM being refilled is obscured.

* A small number of Post Office branches have rear-loading ATM's installed, in which case access is directly within a secure area. If an ATM of this type is installed at your branch the instructions with an asterix in the list above will not apply.

You must make a daily security check on the ATM (see below).

Daily checks on all Bank of Ireland ATMs

You must make a daily check of the ATM to ensure that there have been no attempts to tamper with it.

If you believe that someone has gained access to your code for the combination lock on the ATM safe, you must change the code immediately, as follows:

- Enter 6 x '0's into the code pad
- Enter your existing code
- Enter a new code
- Confirm the new code.

10.2 Internal and external ATMs administered by banks other than Bank of Ireland

The following security standards apply to branches that are authorised to use Post Office cash to fund their ATM. The instructions for daily operation can be found in the user manual supplied at the time of installation.

Security instructions

You must always comply with the following security procedures for this make of ATM:

Your ATM cash holding limit, which you must observe, is determined at the time of installation.
If your ATM is protected by an alarm system, this must be used at all times.
Cash awaiting transfer to your ATM must always remain secured in your main safe.
Other than when you are filling your ATM with cash, the ATM keys must be kept at all times in your main safe.
In the case of Internal ATMs, the cash in your ATM must be removed overnight and the doors of the equipment left open, to show that cash is not stored within the machine; In the case of External ATMs, you should not remove the cash from your ATM overnight, unless you do not have arrangements for a Police response to your alarm system.
Cash removed from your ATM up to a limit of £2,000 can be secured in a retail safe; amounts in excess of this must be secured in a retail safe of a European standard appropriate for the amount of cash being secured.
Access to the ATM must only be permitted out of business hours, or when the premises are closed and no members of the public are on site (this applies to external ATMs when the ATM backs on to the public area of the branch)

POL00423229

When it is fitted, the time delay on the ATM safe must not be started while members of the public are in your branch.
While you are refilling the cash in your ATM, all doors to your branch must be locked and secured to prevent access from the exterior of the premises.
It is recommended that two persons refill the ATM with cash: one person should remain vigilant adjacent to a personal attack alarm button and one should refill the ATM.
You must ensure that any view that the public may have of the ATM being refilled is obscured.

Daily checks on ATMs

You must make a daily check of the ATM to ensure that there have been no attempts to tamper with it.

If you believe that someone has gained access to the code for any combination locks that are installed on your ATM, you must change the code immediately, following the instructions in your user manual.

10.3 ATMs maintained by Cash In Transit (CvIT) crews

You must always follow the relevant security procedures listed below, regardless of whether the Cash In Transit (CvIT) crew maintains your ATM during or outside of normal Post Office opening hours:

Maintenance during Post Office opening hours

- Do not admit the CvIT crew to your branch outside of normal opening hours, whatever the reason
- Ensure that the counter access door and the main safe are kept locked while the CvIT crew are on your premises
- If any CvIT personnel are threatened or attacked while maintaining your ATM, do not put yourself, your staff or your customers in any danger; always summon the Police by calling 999.

Maintenance outside of Post Office opening hours.

Maintenance of your ATM by a CvIT crew outside of Post Office opening hours will always be advised in advance.

If only one person is available to open the door to your premises, an electric bolt may be activated from the secure area to admit the CvIT crew, but you must not rely on this arrangement as a security procedure while the ATM is being funded. The delivery crew must secure the normal door locks as soon as you have allowed them access to the building.

- Ensure that the counter access door and the main safe are kept locked while the CvIT crew are on your premises
- If any CvIT personnel are threatened or attacked while maintaining your ATM, do not put yourself, your staff or your customers in any danger; always summon the Police by calling 999.

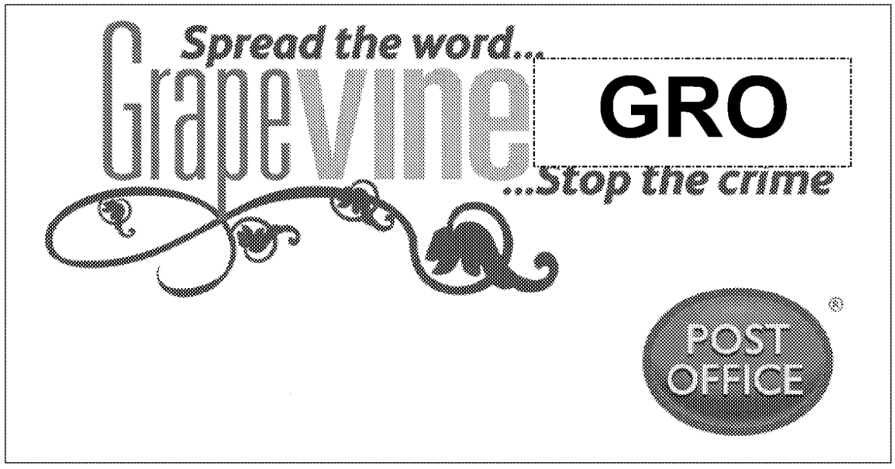
Occasionally a CvIT crew will need to gain admittance to the secure area of your branch to access the ATM safe. In this instance the crew must be clearly identified before access is permitted and they should be escorted at all times while they are in the secure area.

POL00423229

11 Grapevine Intelligence Service

All branches

Post Office Ltd Security, in association with all national Police forces, has introduced a new crime-fighting initiative called Grapevine®, from which all Post Office branches may benefit, as it can provide an early warning of criminals operating in their area. It has already proved effective in the Greater Manchester and Merseyside areas, where it has been operating for some time, but it is also becoming valuable in rural areas, where theft by deception is prevalent.



Grapevine® is a single point of contact for gathering crime-related intelligence on a national local rate phone number - GRO The service operates between 8.00 and 18.00 hours on Monday to Friday (messages are only sent out between these times).

Front line staff can use the number to report suspicious circumstances such as the following:

- people acting suspiciously
- vehicles used for suspicious activities
- product or service fraud
- suspected fraudulent activity, eg, counterfeit notes, suspicious Debit/Credit card transactions

The information can then be shared quickly with other local branches, Police forces and CvIT (Cash in Transit) crews as appropriate.

The National Security Team and/or the Police can then act upon the information and provide the necessary support to branches, with the aim of reducing crime, and its worst effects on staff and business assets.

Any member of staff can register free of charge to receive free text or email messages about suspicious activity in the local area, not just the Branch Manager, the sub postmaster or the franchisee/agent. The more people that register for the service, the more effective the lines of communication are likely to be. All that you need to provide are a mobile telephone number and/or an email address.

However, you do not have to register to report any suspicions you may have on the Grapevine® phone number, so that other people in the business can be alerted to potential criminal activity. This is a vital aspect of the service. Any contact details provided are kept by Grapevine® only.

The provision of this service should not prevent you from dealing with actual criminal activity in the normal way. If you feel at risk from an imminent attack or you have been involved in an attack, you should activate your bandit alarm as long as this does not place anyone in danger. You should contact the Police using 999. Any incidents involving robbery, burglary or theft, or fraudulent activity must be reported to the National Business Support Centre (NBSC).

POL00423229

12 Managing business information

Information is a valuable asset to our Business. It exists in many forms, such as completed applications and transaction details, reports and plans, manuals and email messages. It is communicated by a variety of media: in print, by spoken word, on the Horizon system, by text or phone message, etc. In addition, it can be distributed through different channels; for instance, by post, by computer, by telephone, by fax or text.

The security of all business information is vital if we are to maintain the trust of clients and customers, the company reputation and the value of our brand. Therefore, all Post Office Ltd staff, sub postmasters, franchisees and operators (ie, agents) have a responsibility for ensuring that business information of all types is managed properly and suitably protected, whatever the medium used for its communication, or the means by which it is shared or stored.

This section explains exactly how you must keep confidential information secure in the workplace and prevent unauthorised access to it.

Please remember: Much of the information that you handle will contain details relating to our customers, which must be kept confidential. For this reason, it is your responsibility to protect this information, even when you are disposing of it.

13 Classifying and managing confidential information

Identifying confidential information

In order to fulfil your obligations relating to the safeguarding of information confidential to Post Office Ltd (and to its partners/clients/customers/employees), you must first be confident about identifying information which is confidential.

Post Office Ltd defines confidential information so that it includes any documents, electronic or physical, which contain information about any member of the public, or any employee of Post Office Ltd, or any partner, client or corporate customer of Post Office Ltd, and which are handled or processed at Post Office branches must be regarded as confidential.

The following examples must always be categorised in this way:

- any documents containing customers' or employees' personal information
- forms/applications completed by a customer or by an agent on behalf of a third party (this includes spoiled or discarded forms which have been partially completed)
- customer signatures or card details (eg, those that appear on till receipts)
- all other customer or employee information received in any format (eg, by fax, email or post)
- any data printed from the Horizon system which contains personal data

Storing confidential information

Details about how long official documents must be kept for audit purposes appear in the 'Retention of forms' template in the product and service booklets contained in the Operations Manual. You must not keep confidential information in your branch for longer than is strictly necessary for business purposes.

If the confidential information you are using is a printed copy of information held electronically, you should dispose of the printed copy as soon as you have no further need for it (see 'Disposal of confidential information' on page 37).

If the confidential information is the only record held (eg, because it contains a signature, or because it is not stored elsewhere) then you must ensure that it is kept for as long as it may be required, to answer queries or to deal with any disputes which may arise. In all cases, the need to properly dispose of confidential information must be balanced against the need to keep appropriate records for risk and management purposes.

When confidential information needs to be stored, it must always be kept in a secure location that prevents it being seen, copied or otherwise used by people who have no right to have it; this is unauthorised access. This also means that during office hours you must keep confidential information away from the general public unless it is relevant to the specific customer you are serving (eg, a passport application, a National Savings & Investments application forms, etc).

Once a transaction is completed, any documents containing confidential information must always be placed out of sight of other customers, other staff, engineers or visitors.

POL00423229

Outside office hours confidential information must be stored in a filing cabinet/cupboard/drawer which must be locked, and the key must be kept out of sight and, if possible, in a secure location of its own.

Transmitting confidential information

You must also be careful not to make confidential information available to anyone not authorised to have it (eg, other Post Office staff, engineers, visitors when you are discussing confidential information, such as customers' personal details, or when you are sending confidential documents in the post.

You should not use a mobile phone to discuss confidential information unless it is absolutely necessary. If it is necessary to do so, find somewhere private to talk so that you can not be overheard by anyone else.

If you have to post confidential information, it must be 'double-enveloped' (ie, the confidential details should be placed in a second envelope within the first one).

You must mark the inner envelope 'Confidential' above the written details of the recipient's address.

The outer envelope must bear the recipient's name and address. A return address should be written on the back of the envelope. You must not mark the outer envelope 'Confidential'.

Disposal of confidential information

All branches have been provided with security instructions relating to the disposal of confidential information in the workplace. The following instructions are provided as a reminder. They are mandatory and must be followed without exception:

- Always use a separate bin for confidential information that is being disposed of; ensure that it is clearly marked or colour-coded to distinguish it from the bin for normal waste, and made inaccessible to the general public
- Never dispose of confidential information with your ordinary waste (ie, in ordinary waste paper bins, dustbins or recycling bins/boxes as they could be stolen by criminals and used to commit fraud or identity theft)
- Ensure that you dispose of all confidential information by destroying it in your branch or by passing it to a third party specialist to destroy.

Please note: If you destroy the confidential information in your branch, you must render it unreadable by anyone else by either incineration (not a domestic bonfire), shredding or pulping. The best means of destruction is a cross cut shredder (preferably with a grill size of not more than 6mm).

14 Authorised use of the Horizon system

All staff and/or assistants employed to work in your Post Office branch must be individually authorised to use the Horizon system and its data. They must only use the system and the data contained on it for the completion of official business; otherwise, you and/or they may be committing an offence under legislation such as the Computer Misuse Act (see 'The Computer Misuse Act (1990)' on page 38). Unauthorised computer access may also result in breach of the Data Protection Act, the Theft Act and/or the Telecommunications Act.

Full details of the correct use of Horizon passwords and User IDs can be found in the Horizon System User Guide; Office Administration booklet.

All users of the Horizon system must **never**:

- log on as another person
- allow anyone else to use their User ID and password
- use an informal name, pseudonym or nickname as an identity
- continue to use Horizon or the data on it if you or they are no longer authorised to do so
- allow a User ID or password to be re-used by another person (ie, if you replace a current user with another, the new user must have a completely new User ID and password)

If you need to leave the Horizon terminal unattended:

- Lock the terminal by pressing 'home' and then 'temporary lock'
- Always log off your computer at the end of the day.

POL00423229

The only exception to this is in the event of a fire alarm, when you must immediately follow evacuation procedures without stopping to log off your computer, collect papers or any other belongings.

Password Do's and Don'ts

When you construct a password for use on the Horizon system, you must apply the following instructions:

- Use a mix of upper and lower case letters, numbers, and special characters, if possible (if you use 'London', make it '£oND0n'); make the password memorable for yourself but difficult for others to guess
- Use a password which contains 7 or more characters
- Do not use your first or last name, your login name or your User ID in any format as a password
- Do not use any information about you that is easily obtainable (eg your phone number)
- Never write your password down or share it with anyone else.

Please remember: You are responsible for your User ID and your password. If you think that your password has been revealed to anyone else, or compromised in any way, you must change it immediately.

Full details of the correct use of Horizon passwords and User IDs can be found in the Horizon System User Guide; Office Administration booklet.

15 Security of publications

Operational publications, such as Operational Focus, Operations Manual interim and the booklets making up the Operations Manual contain a wealth of information which is confidential to Post Office Ltd and its clients.

These documents must be treated as confidential information and must always be kept in a safe place in the secure area of your branch, and out of reach of the general public, and other people unauthorised to read the information such as engineers and other visitors. The information given is for internal use within the Business. Under no circumstances should whole documents, or parts of these documents, be shown to, copied for, or given to customers, or anyone else not authorised to have them.

When you destroy any operational publications, you should always treat them as confidential information, and destroy them accordingly (see 'Disposal of confidential information' on page 37).

In the case of branches who receive the Operational Publications CD, you must always destroy versions which you are disposing of by scoring several times across the silver side with either a biro or coin starting at the centre and working out, or bending/breaking the CD in half, taking care not to injure yourself. You can then dispose of the CD in your normal branch waste.

16 Legal guidelines

There is a substantial amount of legislation in operation that applies to the use of information and computers. The legislation holds individuals personally responsible for correct use of systems and for ensuring that they do not breach the relevant laws, it is in your interest to understand those mentioned below in detail:

Data Protection Act (1998)

A leaflet about the provisions of the act was distributed to all branches in August 2006. Further copies are available from Stuart Harvey, the Head of Data Protection Services (Tel: GRO). If you do not comply with the act, and deal with personal data properly, you will be liable.

The Computer Misuse Act (1990)

The Computer Misuse Act 1990 is the principal legislation dealing with the misuse of information systems. There are three offences under the act:

- unauthorised access to computer material
- unauthorised access with intent to commit or facilitate commission of offences
- unauthorised modification of computer material

POL00423229

Official Secrets Act (1989)

In the service of the Post Office, you have signed a declaration that you will comply with the Official Secrets Act. This means that you must keep all relevant information confidential.

Where to get more information

For further information, please contact the NBSC and select option 3.

POL00423229

17 Types of equipment in branches

This subsection identifies the majority of the different types of safe and associated burglary/robbery deterrent that have been installed in branches over the years and provides basic advice on their function and operation.

Post Office Ltd has invested a great deal of money in the provision of this kind of security equipment for the protection of our staff and agents. Using risk criteria, branches deemed to be at highest risk to burglary and robbery receive the highest-grade equipment first. This inevitably means that there are many varied combinations of security equipment installed in our branches throughout the network.

Also because the network is made up of various types of branch, and premises vary with regard to accommodation space for secure storage, the amount and kinds of safes that are fitted in branches will naturally vary.

Therefore, you will need to work out which operational and maintenance instructions apply to your branch from the instructions below by identifying the relevant heading which relates to the sort of equipment installed in your branch.

Please remember: Branch Managers, sub postmasters and managers of Post Office Ltd insured Franchised branches each have an obligation to ensure that the equipment that they have been provided with in their branch operates correctly and is used for the purpose it was designed.
Detailed operating instructions for all equipment provided by Post Office Ltd (including replacement instruction booklets) can be obtained from the NBSC.

In addition, a poster 'Always Alert' (MISC934) that describes the crime-preventing equipment in operation in branches is available from Swindon Distribution Centre and should be used to discourage criminal activity.

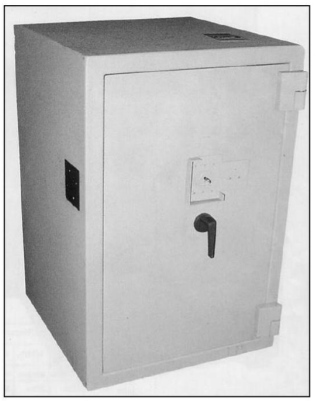
17.1 Types of safes and secure storage available

Please note: Instructions about how to keep cash and stock secure in safe storage can be found in subsection 6; page 19.

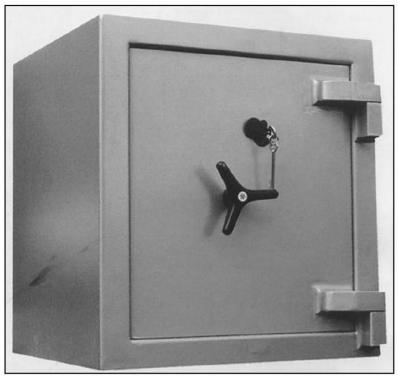
All branches

The illustrations below show the most common types of safes used by Post Office branches. In most instances they are provided free of charge by Post Office Ltd who own them and are responsible for their maintenance.

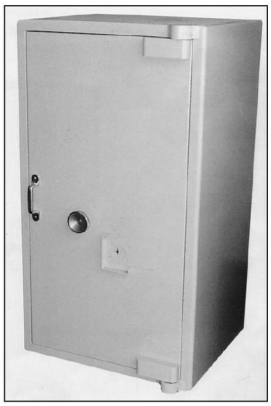
Chubb Conqueror



Community



Grade 1A



POL00423229

SLS

John Tann Clarendon

EFSG

However, there are other types of safe in use, and if you have any queries about these and who owns them, you should contact the NBSC.

The standard terminology that is used throughout this booklet to describe the grades of safe that are used are:

Official safe	any safe used to secure Post Office cash and stock
Main official safe	official safe used to secure Post Office cash and stock but fitted with most items of security equipment (eg Time overlock (electronic or mechanical), time delay lock, time delay compartment, alarm)

Function

The function of the safe is to provide secure accommodation for all of the cash and value stock in your care. It is designed to provide burglary protection outside of business hours and robbery protection during business hours. Many safes, particularly in non-residential branches, are bolted to the floor to prevent them from being removed.

Operation

Safes must be kept locked, with the keys removed, when not in immediate use. Keys must be concealed from public view.

During business hours the safe must contain the bulk cash and value stock, and any other valuable items that are unlikely to be required immediately. Counter staff should normally be provided with cash for one and a half hours' working time, unless there is less time than that remaining until the close of business.

Outside of normal Post Office hours of business, ideally all cash and value stock must be accommodated in a Post Office Ltd main safe, or another safe affording equal protection. If this is not available, alternative secure storage must be used in appropriate priority order, see subsection 6, page 20, 'Standards for secure storage of cash and value stock, etc'.

Any manager or sub postmaster who cannot provide suitable secure storage must use what is available to the best advantage and advise the NBSC or in the case of Crown Offices, the Property and Facilities Helpdesk as soon as possible.

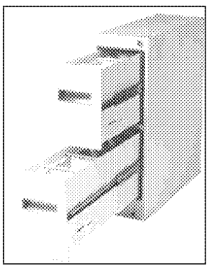
POL00423229

Secure storage other than the main safe

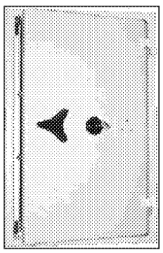
Coin Cabinets

Coin Cabinets are of varying size (see illustrations below).

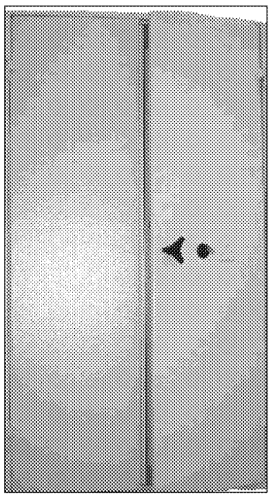
Size 1



Size 3



Size 5

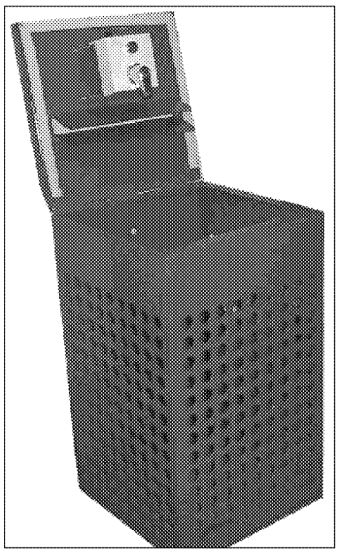


They are installed at branches where additional accommodation is required for the storage of low value coinage and where space is at a premium. Coin Cabinets must be kept locked, with the key removed, at all times when not in immediate use.

Due to the weight of coin placed in these containers, they are bolted to the floor for stability.

Edinburgh Boxes

An Edinburgh Box is a small metal container, which has a slam-shut lid and is bolted to the floor, usually adjacent to the safe (see illustration to the right). It is used for the quick deposit of Cash Remittances.



Just before a Remittance is delivered, you must ensure that the Edinburgh Box is empty. The lid of the box must be raised and the key for the box kept inside the safe that is fitted with a time delay lock.

When the Cash Remittance is received it must be placed immediately in the box and the lid slammed shut. When it is considered safe to do so, the key should be retrieved from the time-locked safe and the remittance pouch should be transferred to the safe.

POL00423229

Branches without counter screens

Roller and Teller Cash Dispensers

Roller Cash Dispensers and Teller Cash Dispensers are security devices that restrict access to banknotes to pre-determined amounts. The decision on which type of dispenser and what level of access to cash is required will depend entirely on the type of business carried out at the branch receiving the equipment.

17.2 Timelocks on safes

All branches

The various types of timelock that have been provided for Post Office safes are illustrated and described below. All of these devices work independently of each other and must therefore be set independently of any other item of security equipment that has been provided at your branch.

When supplied, adhesive labels advertising the presence of time locks must be displayed on the safe door or in another suitable position, if the safe is not visible to customers.

Mechanical time overlock (MTOL)

The MTOL (see below) is fitted to the inside of the safe door and is linked to the door bolting mechanism. Access to the safe (even with the key) is prevented during any period of time when the MTOL is set.

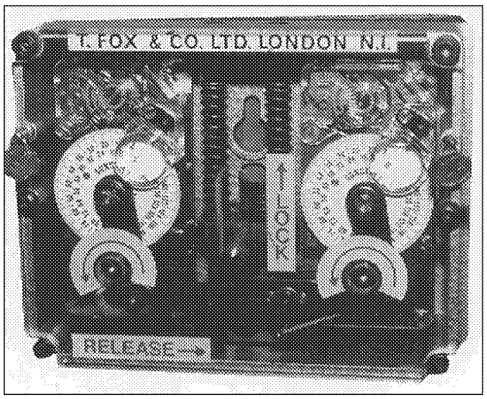
It is designed to deter those kinds of burglary where safe keys are stolen from safe keyholders and hostage situations where sub postmasters and staff may otherwise be forced to open safes outside of business hours.

The MTOL consists of two clocks that operate independently of each other. The clocks can be set in ½ hour increments by means of a key that winds up each mechanism. Usually the clocks are set so that they allow access to the safe no earlier than 30 minutes prior to the official opening time of the branch.

For example: If the clocks were being set at 6pm in the evening and the safe was not due to be opened until 8.30am the following morning, the clock mechanisms would need to be set for 14½ hours.

In the event of one clock failing or being over-set, the other clock would allow the safe to open.

Some branches, particularly if they have a second safe or they can ensure that there is sufficient cash at the counter to meet operational needs first thing in the morning, set the MTOL on the main official safe to open after the branch has opened for business. This ensures that the bulk cash can be kept under time-locked conditions until 30 minutes after the branch has opened for business.

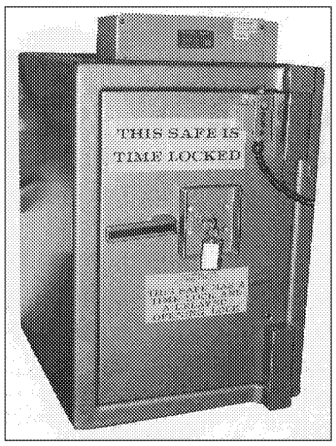


In branches where bulk cash and value stock is locked in the main time-locked safe and there is no operational requirement to access it, the MTOL may be set between 4.40pm and 5.30pm as an extra precaution when the branch is quieter and/ or the evenings are darker.

Please remember: Where an MTOL is fitted, a label advertising the fact should be displayed externally on the door of the safe.

POL00423229

Time Delay Lock (TDL)



The Time Delay Lock (TDL) operates in combination with the standard safe lock. Its purpose is to impose a few minutes delay (normally four but 15 minutes in Northern Ireland), between the key being turned in the lock and the safe door opening.

This is to deter robbers who would be loath to wait four minutes to steal the main cash. It means that the only cash they would have access to would be the 'working cash' (a maximum of 1½ hours operational cash per member of staff), ie the recommended amount that should be in the counter tills at any one time.

Please note: In the case of screen-less branches, the operational limit for working cash is £600.

Operation of the TDL mechanism is automatic and there is no requirement to manually set it. When the safe key is inserted and turned, a red light will be visible. When the delay period has passed and the safe is ready to open, a green light will come on and a buzzer will sound. The majority of these systems are mains powered with battery back up.

Please note: If you have a TDL fitted to your safe, you must not attempt to override this mechanism in any way or keep the safe open with the door bolts extended.
A label advertising the existence of a TDL should be placed externally on the door of the safe.

Time Delay Lock Compartment (TDLC)

The Time Delay Lock Compartment (TDLC), particularly when combined with a time overlock, restricts access to bulk cash to times when the branch is open for business and so deters criminals from robbing branches prior to scheduled opening times. It also provides additional protection from robbery throughout the day.

It is located inside the safe, and is, essentially, a safe within the safe that measures 11" high x 14.25" wide x 15" deep, where bulk cash can be secured. It operates in combination with the time delay lock located on the safe door by imposing a 40 minute time delay before the bulk cash that has been stored can be accessed.

Please remember: Where fitted, the TDLC must be used for the storage of bulk cash at all times.

As much cash as possible must be stored in the compartment at any one time, particularly when the branch is closed. However, during normal hours of business sufficient cash for standard operational needs (ie, no more than 1½ hours 'working cash' per member of staff) may be stored outside of the compartment, in the main body of the safe, with the 4 minute delay facility set.

Please note: In the case of screen-less branches, the operational limit for working cash is £600.

When the main safe door is open:

- Press the red button on the front of the compartment.

The button will be illuminated with a red light to advise you that the 40 minute delay sequence has started.

- Close the safe door, lock it and remove the key.

When the compartment is ready to be opened, the yellow and green lights on the front of the safe will come on and the buzzer will sound.

- Unlock and open the safe door immediately (the inner compartment can then be opened by turning the handle).

If you need to cancel the 40 minute delay sequence:

- Press the gold button on the front of the compartment.

Please remember: If space permits, as well as your bulk cash, you should store in the compartment things like bulk foreign currency, and bulk Postal Orders and stamps.

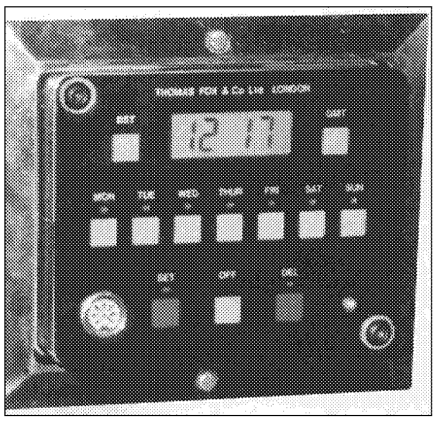
Where a TDLC is fitted, a label advertising the fact should be placed externally on the front of the safe.

POL00423229

Electronic Time Overlock (ETOL)

The Electronic Time Overlock (ETOL) combines the functions of the time delay lock and the mechanical time overlock, and offers the same protection for bulk cash and value stock that the other two devices do individually (see above). It is mounted within the safe door.

The unit is pre-programmed with opening times to suit each individual branch and is operated by simply pressing the 'set' button. An agreed 'latest setting time' is also programmed into the unit and if the ETOL is not set by the programmed time, the system will automatically lock the door mechanism.



There is also a delay (del) button that has two functions:

- to give an extended time delay period (eg for use during lunchtime closures)
- to delay the automatic setting time, in increments of one hour, (if required in the evening)

Where an ETOL is fitted, a label advertising the fact should be placed externally on the door of the safe.

Insafe Mk I Electronic Time Overlock (ETOL) or Matrix Multigard (MMG)

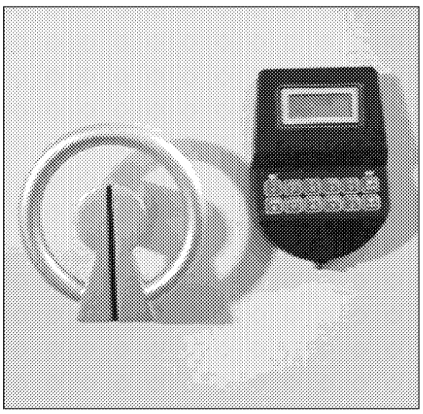
The Insafe Mk 1 ETOL and the Matrix Multiguard (MMG) combine the functions of the time delay lock and the mechanical time overlock. Whichever is used, it is mounted within the safe door with an external keypad that is operated by a six digit code.

The protection these two devices offer is the same as that provided by the mechanical time overlock and the time delay lock (see above).

The MMG also includes the following features:

- the option to change your PIN code on a regular basis (daily if required)
- an 'open period' time lock extension for late closure (the locking of the safe may be delayed for periods of 30 minutes (up to a maximum of four times)
- an immediate time locking facility which allows you to bring forward your closing time, for early closures (in this case you can unlock the safe at the next open period available, normally the next working day)
- a temporary time lock which allows you to set a temporary 'closed period' up to a maximum set period of 60 minutes (ie, suitable for a lunch period)

* Press any button to start the lock operating.



To open the main safe door:

* Press the 'Main' button.

After four minutes you will hear an audible bleeping and you can then insert the key in the safe door and open the safe.

If your safe has a time delay lock compartment (TDLC) fitted as well:

* Press the 'Inner' button.

After 40 minutes you will be able to access the main safe by pressing and holding the button on the black box attached to the TDLC until the green LED light comes on.

When the light comes on:

* Release the button and open the TDLC.

You can change your PIN code, start the time lock 'open period' extension, and set the immediate time lock or the temporary time lock by using the six digit code provided. Full instructions for this are provided to branches following each installation.

POL00423229

If your safe is situated in a position where the audible 'double bleep' alert when opening the safe cannot be heard, a supplementary silent vibrating 'down timer' alert is provided. You should refer to the instructions provided with the unit.

Please note: If you are unable to 'time lock' your safe due to a mechanical failure, you must inform the NBSC as soon as possible.

17.3 Burglar alarms

All branches

Post Office Ltd deploys several types of burglar alarm at its branches. Each branch should have a set of instructions available, which are specific to the type of alarm installed and which must be strictly followed.

Each person who is permitted to set the alarm (when the system permits, eg, Europlex, Galaxy) must have their own code which must not be disclosed to anyone else. If you believe that someone has gained access to your code, you must change it immediately. In addition to this, all codes must be changed at least every three months.

All alarms (with the exception of remotely monitored alarms) must be tested weekly and a manual record of the test must be kept for audit purposes.

The weekly test must consist of:

- the time and date of the test
- the results of the test
- the initials of the person testing the alarms

Remotely monitored alarms

If your alarm is remotely monitored, you must take every precaution to minimise false alarms. The Police have very specific penalties that they impose in the case of false alarm management. The consequence of exceeding their acceptable level of false alarms is blacklisting and a withdrawal of response by the Police.

You must have at least two key holders who live within 20 minutes of the branch, who are trained to operate the alarm and that have access to all relevant parts of the premises.

Please note: Remotely monitored alarms **must not** be tested weekly as this would amount to a false activation at the Alarm Receiving Centre.
It is vital that you advise both the Police and the Alarm Receiving Centre on GRO of any changes to key holder details. You must also advise the Alarm Receiving Centre if you are going to open or close outside your normal business hours and of any changes to key codes.
Contact the Romec National Service Centre for all system queries, faults or training requirements on GRO

Alarm call-outs

If you are involved in an alarm call-out, you should always take special precautions to ensure your personal safety as follows:

Beware of telephone calls where the caller claims to be a Police officer
Never visit a branch out of hours without first checking the validity of the caller
Never call back using the number given by the caller, always check the number yourself
If you have to visit a branch, tell someone where you are going (if possible get someone to accompany you and ask the Police to attend)
Never take any safe keys with you

POL00423229

Bandit alarms

Bandit alarms may vary from branch to branch as there are a number in use.

Hand-operated bandit alarms are activated by simply pressing them. The reset mechanism is usually a key. The key must never be left in the reset switch.

Foot alarms are operated by standing on them. Resetting is by means of a switch located under the top cover.

Dual -push alarms are the latest technology and meet the latest guidelines. Two fingers are required to operate the two red buttons that must be depressed simultaneously to trigger the alarm. Resetting is either by key or by control panel.

The decision on whether or not to sound a bandit alarm is left to the sole discretion of the staff or sub postmaster. The safety of all staff, sub postmasters and agents, and customers must come first. Post Office Ltd recommends that in potential robbery situations, the bandit alarm should be activated provided that no one is placed in danger by doing so.

Please note: Bandit alarms on non-monitored systems must be tested weekly.

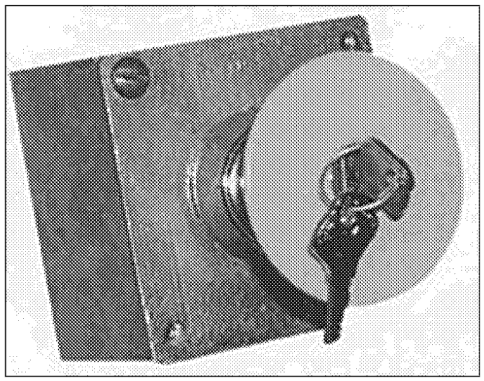
Audible alarms

The purpose of the audible bandit alarm (also known as the personal attack alarm) is to alert members of the public to the fact that there is a potential criminal incident occurring at your branch, so that they can provide useful witness statements or call the Police.

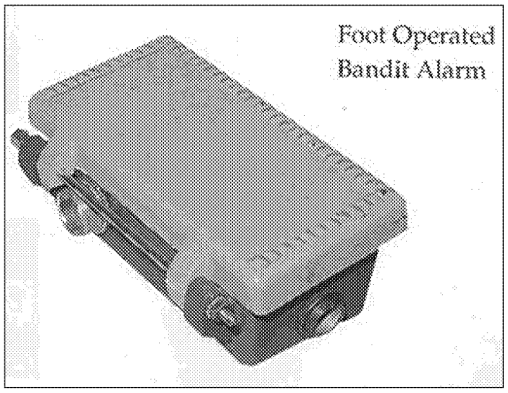
You may sound the alarm if you are suspicious of anyone acting strangely in your premises. The sounding of the alarm is usually sufficient to deter any potential robbery from taking place. Analysis of previous incidents has shown that when the bandit alarm is activated and staff members immediately drop to the floor, the attacker usually leaves the branch.

Please note: You must not, however, sound the alarm in the case of anyone acting suspiciously if your alarm is remotely monitored as this may result in an unnecessary Police call-out.

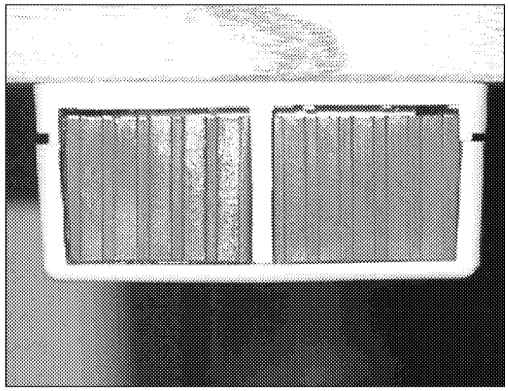
Hand operated alarm with key



Foot operated alarm



Dual push alarm



POL00423229

Silent alarms

At branches where Alarm 2000 has been installed with remote monitoring, silent bandit alarms are linked to a monitoring station.

Extreme care must be taken with silent alarm systems, however, as excessive false activations will result in the Police failing to respond.

Please note: Bandit alarms on monitored systems are 'self-checking' and must not be tested.

Crown Offices and Sub Office branches

EA2K (European Alarm 2000)

This system has been introduced in both Crown Offices and sub post offices from October 2005 to meet new European standards for alarm systems and changes in ACPO (the Association of Chief Police Officers) policy.

The equipment is normally fully monitored by the Alarm Receiving Centre (ARC), using existing telephone lines whenever possible, and the annual monitoring charges are borne by Post Office Ltd. For this reason, if the system is connected to the official Post Office telephone line, the line must be kept free of any personal equipment such as computers, fax machines etc, when this type of equipment would affect the monitoring connection.

The system protection is very similar to that of the Alarm 2000 system with personal attack, safe and perimeter alarm protection.

Operation

The same operational standards apply as for the Alarm 2000 system (see 'Alarm 2000' on page 51).

The main difference is that keyholders/operators now have a key fob to set and unset the system. Full instructions for setting and unsetting the safe using the key fob or code are also provided in the system manual.

The key fob is a security item and must be kept secure and separate from the safe keys. If a key fob is lost or stolen, you must contact Romec to have the fob removed from the system and to arrange for a replacement.

Changes in the ACPO (the Association of Chief Police Officers) policy on responding to false alarms were introduced in October 2005. The changes include a stricter limit on the number of false calls they will allow before the facility of a Police response is removed. For this reason, you must take due care and follow carefully the instructions for setting alarm systems.

Since most false alarms occur as a result of poor opening and closing procedures and the misuse of personal attack alarms, please remember that personal attack alarms must only be used when Police assistance is required. In addition, premises must be fully checked to ensure that they are properly secured before you leave the building, and opening and closing procedures must always be followed as laid down.

Sub Office branches

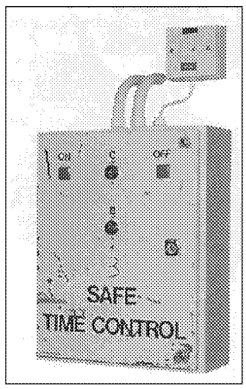
W77, 26L, 26L4, 26L4 (Mk7)

While there are slight differences in the make-up of these alarm systems, their function, operation and maintenance are so similar that they can be considered under one heading.

They are not being installed any longer as they do not comply with current regulations relating to alarm systems. If you have any of these alarm systems currently and it becomes beyond repair, or requires removal for any reason, it must be scrapped and replaced with the new European Alarm 2000 system.

POL00423229

W77



26L4

26L2

26L4 mark7

These systems provide alarm protection to the safe by means of a magnetic 'limpet' which is placed over the safe keyhole when the alarm is being set. If anyone attempts to remove this limpet or to attack the safe when the alarm is set, the alarm will activate.

The alarm is designed to give special protection during lunchtime closure and at night.

If you have this system, when you close your branch in the evening (or at lunchtime) you should carry out the following procedure:

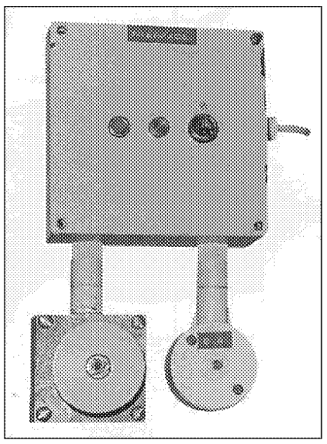
- Place all your cash and stock in the safe
- Lock the safe
- Remove the limpet from its holding plate and place it in the appropriate slot on the safe door
- Switch the alarm on with the key provided (each system is switched on using a different method).

To switch off the system:

- Carry out this process in reverse, ensuring that the time-controlled period has expired before you do.

POL00423229

Interconnection unit



If your branch is equipped with a W77, 26L2 or 26L4 alarm system, it is likely that you will also have an interconnection unit installed. The purpose of the unit is to link the alarm system and the bandit alarm together to enable the internal and the external bells to sound simultaneously whenever the bandit alarm or the alarm system is activated. Normally you will not need to touch the unit.

Keys for the unit (identified by red plastic covers) must not be left in the key switch; they must be kept with the burglar alarm 'B' key. If someone tampers with the system or if there is a fault, the key can be used to silence the internal bells only, as follows:

- Insert the key into the key switch and turn it to the ON position (90 degrees clockwise).

The key will be trapped in this position, the red lamp will remain on (indicating that a fault exists) and the external bell will continue to ring.

- Send for a RoMEC engineer to rectify the fault.

Europlex

As the Europlex alarm system no longer meets the standards necessary to comply with ACPO (the Association of Chief Police Officers) guidelines, if any existing Europlex system becomes irreparable, or requires removal for any reason, it must be scrapped and replaced with the new Alarm 2000.

The system provides alarm protection to the safe and perimeter protection to the premises by means of a seismic key flap which is placed over the safe keyhole when the alarm is being set and by the addition of passive infra-red detectors, door contacts etc, to vulnerable areas. Attempts to move the key flap or the triggering of detectors or door contacts etc, during periods when the alarm is set will result in the alarm activating. When these systems were installed, sub postmasters also had the option of extending the basic system to other areas of their property at their own cost.

The alarm is designed to give special protection during lunchtime closure and at night.

If you have this system, when you close your branch in the evening (or at lunchtime) you should carry out the following procedure:

- Place all your cash and stock in the safe
- Lock the safe
- Place the key flap over the lock on the safe door
- Switch the alarm on with the numerical code provided.

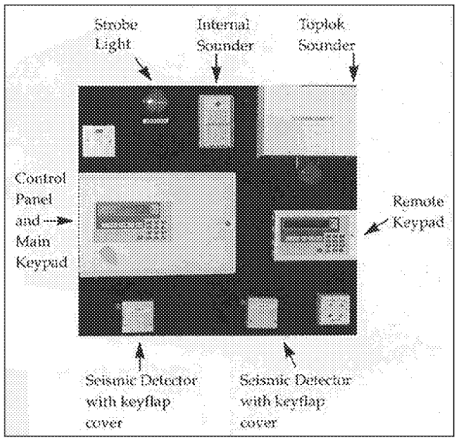
To switch off the system:

- Carry out this procedure in reverse, ensuring that the time-controlled period has expired before you do.

You should also carry out a regular check of the system to ensure that none of the detection devices are being obscured in any way.

This system can also be monitored via an Alarm Receiving Centre (ARC). However, as this system is no longer ACPO approved, no further monitoring arrangements can be made further to those already in place.

Please note: You must remember to advise both the Police and the Alarm Receiving Centre (if appropriate) of changes to key holder details.



POL00423229

Alarm 2000

The Alarm 2000 is a monitored alarm system that complies with ACPO (the Association of Chief Police Officers) guidelines, and branches with the alarm must conform to ACPO policy.

The system is fully monitored by the Alarm Receiving Centre (ARC), using existing telephone lines whenever possible, and the annual monitoring charges are borne by Post Office Ltd. For this reason the official Post Office telephone line must be kept free of any personal equipment such as computers, fax machines etc, when this type of equipment would affect the monitoring connection.

Identified faults on telephone lines must be reported to the Alarm Receiving Centre (ARC).

Sub postmasters are expected to provide the contact details for two key holders who would be able to visit the branch in the event of a valid alarm activation, also to carry out a regular check of the system to check that none of the detection devices are being obscured in any way.

Please note: You must remember to advise both the Police and the Alarm Receiving Centre (if appropriate) of changes to key holder details, and any use of the safe outside normal hours of business.
You must also minimise false alarm activations, otherwise the Police may withdraw their response to potential emergency situations.

The system provides the following benefits:

- daytime protection for the main safe which is fully monitored by the ARC, with times for permitted access, means that you must keep it alarmed throughout the day
- night-time intruder protection including a final set button by the exit door, a set-up where more than one detector must be activated before the alarm will signal to the alarm receiving centre, and remote reset

Operation

If you need to open the safe during the day to obtain cash or stock:

- Unset the alarm by entering your code
- Unset the safe by entering your code, then 'ENT', then '6'
- Reset it immediately you have obtained the items you need.

Please remember: When not in immediate use the safe must be kept in alarmed condition.

When you close your branch at the end of your normal hours of business (or at lunchtime):

- Always place your cash and stock in the safe
- Lock the safe
- Place the keyflap over the lock on the safe door
- Set the alarm by entering your code, then '0'
- Set the safe by entering your code, then 'ENT', then '6'.

Portable panic alarm (Skyguard Mobile Lone Worker Protection System)

Network Outreach services and other branches as specified

The Lone Worker personal alarm system (Skyguard) enables the user to raise an alarm discreetly without compromising their personal safety.

The situations that may require the use of a Lone Worker personal alarm system are:

- the provision of a Mobile Core and Outreach service
- the provision of a Hosted Core and Outreach service
- the provision of a HomeService Core and Outreach service
- when a risk assessment has shown that the installation of a lone worker alarm is justified

It consists of an alarm device, similar to a small mobile phone that can be worn discreetly on a belt or a lanyard, and which must be carried by the user during all periods of operational activity.

POL00423229

The device uses mobile phone technology and Global Positioning System (GPS) satellites to accurately send details of location to the ERC (Emergency Response Centre). It is designed to be activated when the wearer feels that they are under threat of an attack or when an attack has occurred.

Alarm buttons on the unit discretely activate the lone worker alarm, sending its location to the Skyguard ERC followed by a silent voice call.

Two way voice communication then allows the ERC operator to listen to an incident discreetly without putting the user at any further risk, and to talk to the user if it is safe to do so to gain further information. The operator will rule out the possibility of a false alarm before calling the appropriate emergency service. All conversations are recorded and kept on disc for auditing or post incident use.

Users of the system receive training on its use prior to deployment and in accordance with the following instructions which must be followed on a daily basis.

If the Skyguard 500 Personal Safety Device malfunctions or you have an operational question:

- Please contact the Skyguard Help Desk on GRO

The Help Desk is open on Monday to Friday from 0900 to 1800 hours.

Getting started (initial set-up)

For information on the initial set-up activation call, see pages 12 and 13 of the personal alarm User Manual supplied with the device.

- Please ensure that your personal details are entered and updated as required on the Customer Control Panel (CCP). All updated information is managed by the Post Office Ltd Equipment Team (on GRO
- Ensure that the personal alarm is charged for a minimum of 8 hours a day and that the green GPS LED is on and not flashing; if it is flashing, take the device out into the open air and hold it up towards the sky until the GPS light stabilises
- Press and hold the 'Call' and ERC buttons simultaneously for two seconds.

The green 'Sending' LED and red SOS LED will light up. After a short time (normally 25-35 seconds), you will hear a beep to advise you that the PSD has connected to the Skyguard Emergency Response Centre (ERC) and that the operator is listening.

- When you hear the beep, say 'Activation call, Activation call'.

The operator will ask you one or two questions based on your user details and confirm your location.

Daily use

The personal alarm device should be kept switched on at all times as this helps to maintain an accurate and fixed link to the Global Positioning System (GPS).

If you do need to turn off the device for any reason, you should follow the instructions below:

To turn off the device:

- Press and hold down function buttons 1 and 3 simultaneously for two seconds.

POL00423229

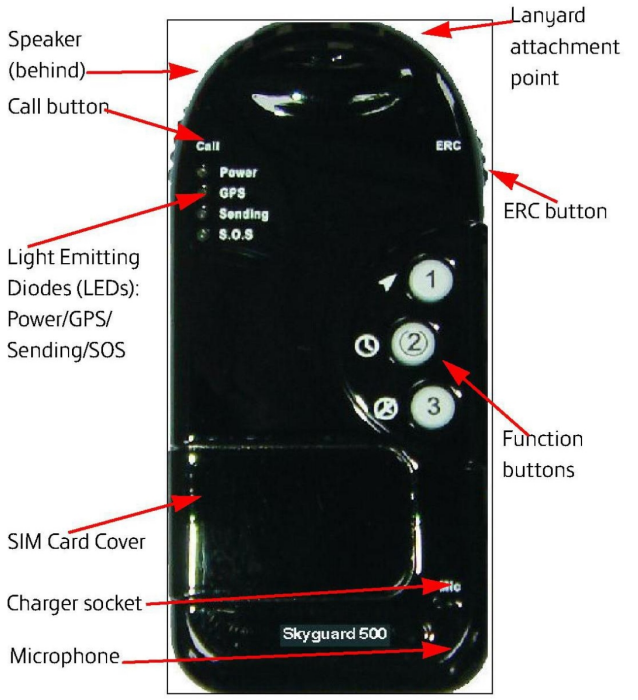
To turn on the device:

- Press and hold down the function button 2 for two seconds.

The power LED will then come on.

When the device has been turned back on, you should ensure that you have a current link to the the Global Positioning System (GPS) before use.

A flashing GPS LED shows that the device does not have a current link to the Global Positioning System (GPS). However, the device will remember and report its last known link, for instance, if you are in a building, it will typically give your position as outside by the front door.



Genuine alarm activation

If you find yourself in a situation where your personal safety is threatened:

- Press and hold the Call and ERC buttons simultaneously for two seconds
- Do not say 'Activation Call' when you hear the beep.

The operator will listen in and assess the situation and start the appropriate escalation process.

- Speak to the ERC operator only if it is safe to do so.

Test GSM coverage

- Press and hold down the function button 2 for two seconds.

THE LEDS will light up to show how good a GSM signal the device has. The more LEDs that are lit up, the stronger the signal is. After a few seconds the LEDs will revert to their normal display.

POL00423229

Additional features

Your Skyguard 500 contains the following features that should only be used in exceptional circumstances as detailed in the tabled guidelines below:

Send Position Report
• Press and hold down the ERC button and function button 1 simultaneously for two seconds. You will hear a voice message confirming that a message has been sent. This will send a position through to the control centre's database which shows you were in a particular place at a particular time. ***Please note:*** This function should only be used in exceptional circumstances. when instructed by Post Office Ltd.
Record Memo
• Press and hold down the Call button and function button 1. This will connect you after a few seconds to the Skyguard Memo Service. • When prompted, leave a short message/memo after the tone. This can be useful if you know you are being called to a particular event or going to an area where a signal will not be strong, eg, a cellar. The memo will become available to the operator only if you subsequently activate the alarm. ***Please note:*** This function should only be used in exceptional circumstances, such as when you feel vulnerable at a site. • Press button 3 to end the call.

To set the Timer

- Press and hold down the ERC button and function button 2 simultaneously for two seconds.

This will set the timer for 30 minutes. If it is not cancelled, the alarm will automatically activate.

To cancel the Timer

- Press and hold down the ERC button and function button 3 simultaneously for two seconds.

The timer is useful if part of the area you work in does not receive good GSM coverage. Before entering this area, you should set the timer in case activation is required. The timer will alarm if not cancelled within 30 minutes.

To call the Help Desk (if appropriate)

- Press and hold the Call button and function button 3 simultaneously for two seconds.

You will hear a voice message confirming that the number has been called.

To receive calls

- Press and hold function button 3 for two seconds.

To end calls

- Press function button 3 again for two seconds.

17.4 Anti-bandit screens

Sub Office branches

A variety of anti-bandit screens (see para 4.2, page 16) are used in Sub Office branches.

The ISIS Project Screen 2000 remains the property of Post Office Ltd for a period of 14 years from the date of installation and Post Office Ltd are responsible for the maintenance during that period. After 14 years the screen becomes the property of the sub postmaster who then becomes responsible for all maintenance issues.

POL00423229

Where a Swindon screen is installed, the glass of the screen should extend 1982mm above the counter or to within 225mm of the ceiling, whichever is lower.

When anti-bandit screens are fitted, there must be no open access into the secure counter area (eg, no gap at the side of the screen or at the side of the door). Where appropriate, extension panels of the glass must be fitted over the screen door and parcel hatch (unless these areas are filled in with another appropriate material) and be securely fixed, and the screen supports should be extended to the ceiling and the gap between the screen and ceiling filled in.

The responsibility for ensuring that there are no gaps providing easy access into the secure area rests with the sub postmaster.

The sub postmaster must keep the anti-bandit screen in a good state of repair at all times. The screen must be kept clean and free of posters that may obstruct the view into the customer-side of the premises.

Please remember: With the possible exception of a few privately installed proprietary screens, no glazing forming part of the anti-bandit screen is ballistic-resistant. However, the counter base of Screen 2000 is ballistic-resistant to G2 standard.

Crown Offices

All Anti-bandit screens (see para 4.2, page 16) at Crown Offices are the property of Post Office Ltd.

When anti-bandit screens are fitted, there must be no open access into the secure counter area (eg, no gap at the side of the screen or at the side of the door). Where appropriate, extension panels of the glass must be fitted over the screen door and parcel hatch (unless these areas are filled in with another appropriate material) and be securely fixed, and the screen supports should be extended to the ceiling and the gap between the screen and ceiling filled in.

The Branch Manager must ensure that the anti-bandit screen is kept in a good state of repair at all times. The screen must be kept clean and free of posters that may obstruct the view into the customer-side of the premises.

Please remember: No glazing forming part of the anti-bandit screen is normally ballistic-resistant.

17.5 Camera systems

All branches

Closed Circuit Television (CCTV) systems

The CCTV system (see below) has predominantly been installed at Crown Offices, although it has also been installed at very high-risk sub Post Office branches.

A videotape system is provided, with 31 tapes that must be rotated on a daily basis and changed every six months so that you retain decent picture quality.

A new videotape must be inserted into the video recorder each morning prior to the start of business, as the CCTV system is designed to operate throughout your normal business hours and maintain continuous videotaped recordings of everything that has happened within the viewing range of the cameras. You are not expected to watch the monitor(s) permanently; the value of this system as a deterrent to shoplifters is, therefore, somewhat limited.

The main purpose of the CCTV is to provide pictorial evidence of any crime that may have occurred within view of the cameras. So you must ensure that the cameras are not obstructed in any way.

Where cameras are fitted, staff and sub postmasters must familiarise themselves with the booklet 'Camera Surveillance - A Guide for Outlet Managers'. This covers identification, record keeping, handling of evidence, the placing of signs and your responsibilities under the Data Protection Act.

Videotapes are usually played via time-lapse video recorders. Replacement tapes are available from RoMEC Services.

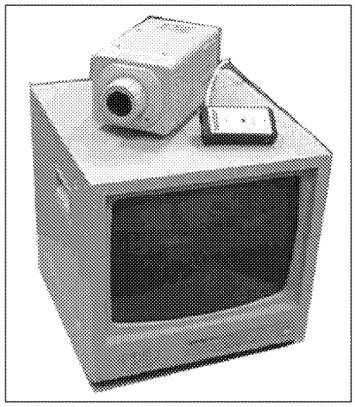
POL00423229

Digital cameras

This camera continually takes pictures of the exit route from your branch. In the event of a robbery or suspicious situation you can store pictures of criminal suspects for later analysis. The camera will store a sequence of images from a time 35 minutes before it is triggered until 10 minutes after.

The camera can also store single images of suspicious persons if required.

Under normal circumstances, the camera operates 24 hours a day and needs no regular attention.



In the event of a criminal incident occurring:

- Trigger the camera by pressing the two side buttons of the camera control unit together, no later than 30 minutes after the incident.

Please remember: You may press the buttons during the incident if it is safe to do so without putting yourself or others at risk.

After 10 minutes the camera will stop automatically; the green light on the camera and the red light on the control unit will flash.

- Contact the NBSC who will arrange for an engineer to visit the next working day, recover the pictures and reset the camera
- Verify the identity of the engineer by telephoning CASE Security on 0870 241 5040.

In the event of a suspicious person in your branch:

- Take single shots by pressing the end button once when the suspect has left the counter and is walking towards the exit
- If circumstances permit, hold the button down until the subject has left the premises. The camera will store images only while the button is depressed
- Note the details such as the description of the subject, the time and the date so that you can inform the person who requested the image.

The images are stored in the camera until required. The camera will still be available to capture other incident pictures, while they are stored.

Please note: The NBSC must sanction any requests you may receive from the Department of Work and Pensions to capture images of suspected fraudsters in view of the need to recover the costs associated with processing the images.

You should maintain your digital camera, so that it continues to operate effectively, in the following way:

- Check daily to ensure that the camera light is on, not flashing (if the light is flashing, contact the NBSC)
- Keep the route to the control unit buttons clear for ease of access
- Check that the camera field of view is not obstructed
- Check that your normal shop lighting is working correctly
- Check that your 'Cameras in Use' sign is in place
- Keep a record of any pictures that are taken, any problems you have with the camera and any engineer visits.

Sub Office branches

35 mm still camera system

This camera takes a series of 200 still photographs in the event of a criminal incident occurring at your branch. The system comprises a camera, a controller unit and activation devices.

POL00423229

It can be operated by two methods:

- by sounding the bandit alarm, you will automatically trigger the camera operation
- by pressing the blue button located on the counter, you can take pictures silently

In the event of a robbery you should always carry out the following actions:

- Run the film through to the end and remove the cassette in the presence of a Police officer
- Complete a Certificate of Transfer and send the film to the laboratory for processing in the envelope provided.

Please note: The Certificate of Transfer is included in the pack that contains the camera and the operating instructions.

- Fit your reserve cassette into the camera and reset the system.

Please remember: When you despatch your film for processing, you must ensure that you include your Post Office (FAD) code, and your full address and postcode on the cassette so that a replacement film can be sent to you by return post.

In order to effectively maintain this type of camera, before the start of **each** business day:

- Test a different one of your camera triggers by setting the key switch to test (to disable the camera when activating the trigger) and activating the device
- Check the Input status light comes on, then reset the trigger
- Turn the key switch back to ready.
- Take two test shots using the camera control box by pressing the 'test' button twice
- Confirm the 'frames used' counter total increases by at least two
- Check that the time is correct
- Check that the date has switched over correctly and shows the correct part of the day, ie AM/PM (refer to your clock manual instructions if any adjustments are required)
- Check that the 'Security Cameras in Use' sign is in place and visible to the public (this is a legal requirement)
- Check that there are no obstructions in front of the camera, ensure that it is pointing in the correct direction and that there is no dirt on the lens cover
- Check that the normal ceiling lighting is all on and there are no defective lights
- Ensure that no unauthorised persons have interfere with the camera controller button.

Please remember: When cameras are fitted, staff and sub postmasters must familiarise themselves with the booklet 'Camera Surveillance - A Guide for Outlet Managers'. This covers identification, record keeping, handling of evidence, the placing of signs and your responsibilities under the Data Protection Act.

POL00423229

17.6 Electric door bolts and Maglocks

Sub Office branches

Electric door bolts and Maglocks have predominantly been provided at branches operated by one person.

Electric door bolt

The electric door bolt is designed to allow you to secure or release the public entrance (or shop) door from the protection of the counter area. This form of security is useful if you think that there is a possibility that you may be subject to attack when you open or close the branch to the public. The bolt is thrown temporarily so that you can secure or release the other locks on the door in safety.

However, you must not use the electric door bolt to stop an attacker from leaving your branch, as they may turn on you.

Where the electric door bolt has been installed, the sub postmaster must ensure that a suitable automatic door closer is fitted and maintained to a high standard at their own expense. The door must also be a good fit within the frame. If the electric door bolt is in working order but will not lock the shop door because the door is ill-fitting or has dropped, the responsibility for repair of the door rests with the sub postmaster.

The electric door bolt must be used to secure the public entrance door before you leave the counter to either secure, or release the other locks and bolts on the door. As soon as this is done, you should release the electric door bolt by means of the control unit behind the counter.

- Do not leave the bolt on for extended periods, as this will cause it to overheat and burn out.

At closing times:

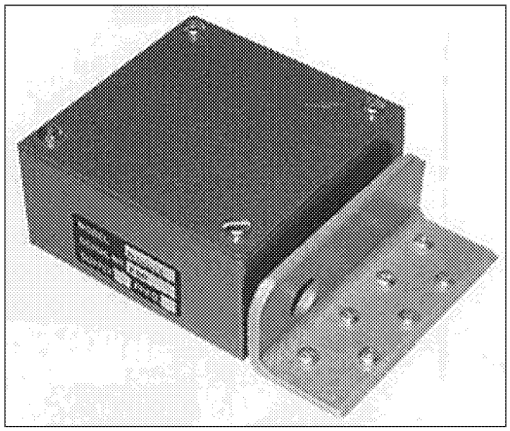
- Check that the door is properly closed before you operate the bolt and before you leave the counter area
- If you cannot see the door from the counter area or the door is not closed, ask your last customer to close it.

To bolt the door:

- Throw the switch to the operated position (the buzzer sounds when the bolt is fully extended).

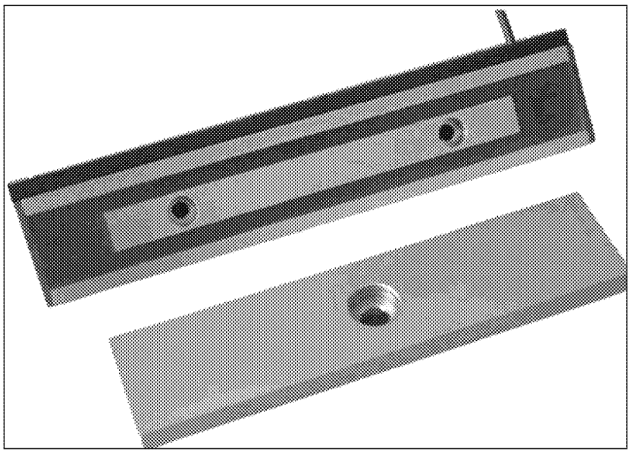
To unbolt the door:

- Throw the switch to the opposite position (the bolt will retract and the buzzer will cease).



Maglock

Maglocks differ from electric door bolts only in that they use a magnetic contact to secure the public entrance (or shop) door rather than a bolt. Maglocks are in limited supply and have only been installed on doors where the installation of an electric door bolt was not possible.



POL00423229

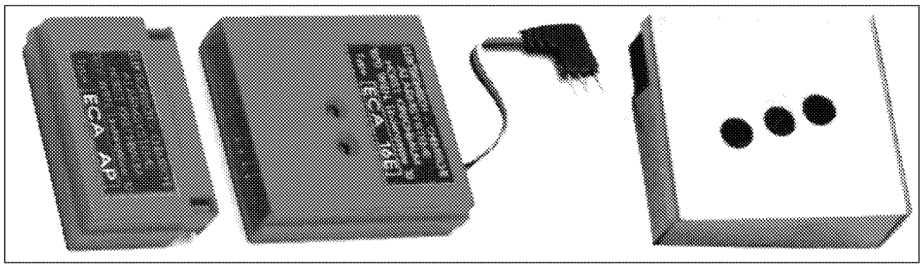
17.7 Smoke and Dye devices

All branches

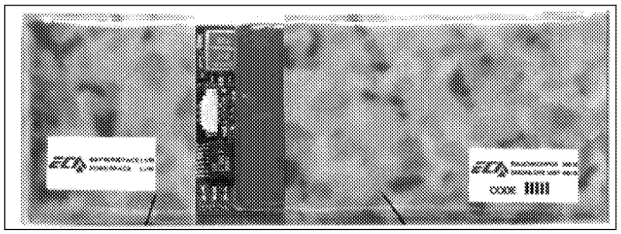
There are two types of Smoke and Dye device in operation and a combination of these devices is usually provided at branches where Smoke and Dye is installed:

- the 16E pack which is concealed in a bundle of £20 notes
- the Smokenote™ which is made to resemble a single £20 note

16E pack



Smokenote™



The Smoke and Dye device is planted amongst a number of genuine banknotes and is designed to provide a deterrent to robbers who attempt to steal cash from your branch in the following way:

You should remove the Smoke and Dye devices from the safe at the start of business and keep them in a counter drawer throughout the day. If a robbery takes place in your branch, you should hand the Smoke and Dye devices to the robber with any other cash that they demand.

Please note: You must not remove the Smoke and Dye packs from the designated secure counter area.

The device activates a short way from Post Office premises causing all stolen banknotes to be marked with red dye. Passers-by are also made aware of the incident as the devices issue red smoke. Usually the bag containing the stolen notes is left behind as the criminals attempt to make good their escape.

The devices must be kept with the working cash on the counter during business hours and secured in the safe each night. The only exception to this is where branches have received written authority to keep the devices in the counter drawers overnight. Written authority will only be provided where the layout of the branch is such that the devices are likely to activate if they are placed in the safe.

On installation, you will need to provide the engineer with genuine banknotes from Post Office funds. He will glue four x £20 banknotes to each 16E pack installed and two x £20 notes to each Smokenote™ installed. The engineer will also request a varying number of other £20 notes to be wrapped around the Smokenote™ using an elastic band. The serial number of each banknote must be noted and a record maintained of the total amount of cash used to make up the Smoke and Dye devices. You must account for this cash as cash-in-hand on each balance you complete.

In order to ensure that Smoke and Dye devices are operating effectively you should carry out the following checks on a daily basis:

- Check that the Smoke and Dye packs are ticking
- Check that the start transmitter at the public entrance door is showing a green light.

POL00423229

17.8 Cash Carrying Cases

Network Outreach services

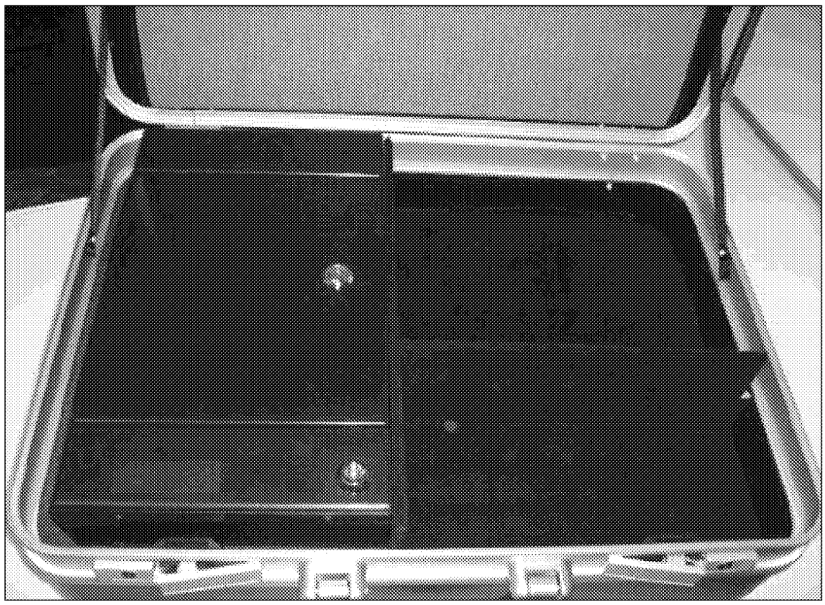
Two Cash Carrying Cases with a dye degradation system are in operation for Network Outreach services:

- the 'Proxima' security case with a maximum cash holding of £6,000
- the high value IBIS security case with a maximum cash holding of £15,000

Each Network Outreach Service provider will use the case that is appropriate for the value of cash that is being transported and the level of security risk attached.

Proxima security case - instructions for use

The 'Proxima' security case is illustrated below.



Please note: It is strictly forbidden for anyone to operate the case unless they have been fully trained, and have signed and dated the relevant handover document.

To arm the case:

- Always switch on the proximity transmitter before arming the case alarm
- Place the unwrapped cash in the inner cash compartment and lock the compartment
- Place other value stock and items for secure storage during transportation in the main compartment of the case
- Press and hold the On/Off button on the front of the proximity transmitter for four seconds until the green power light and the red transmit data light come on
- Release the button (the red light will flash intermittently for about five seconds
- Turn the key switch to the test position on the case alarm unit (the blue 'receive data' light will flash and the on board sounder will chirp every six seconds in the test mode
- After testing turn the arm key switch to position 4 'Arm Siren/Ink' (with the proximity transmitter switched on, the on board sounder will chirp five times to indicate that the system is armed; the blue 'receive data' light will flash intermittently)
- Remove the arm key and the cash compartment key

POL00423229

- Close and lock the lid with the case key and keep this separately in a secure place.

Please note: Please keep all keys separately.

Transporting the case

- Anchor the ripcord safety plu into the vehicle and insert the jack plug into the case.

Please remember: The case should be transported in the passenger footwell or behind the front seats.

Upon arrival at the Network Outreach site

- Always take the case into the premises first; keep the proximity transmitter on your person and left turned on (the case can then be safely left while you collect other items from your vehicle and will not activate unless it is moved)

Please note: The alarm keys can only be removed in the 'Armed' position.

- With the proximity transmitter still switched on, unlock the lid of the main case and remove the 'working' stock
- Leaving the case armed, unlock the inner cash compartrment and remove the 'working' cash
- Relock the inner compartment and the outer lid
- Place the case in a secure location where it will not be moved
- Push the button on the proximity transmitter for four seconds to turn the case off

- Do not move the case
- If you need to reopen the case to remove more cash or stock, switch on the proximity transmitter by pushing the button for four seconds - the case can then be opened.

Please note: If you open the case while the proximity transmitter is switched off, the movement will sound the alarm and begin the activation mode. This mode lasts for 15 seconds. to stop the activation of the case, do not move the case and it will automatically reset. Alternatively you can switch on the proximity transmitter.

To disarm the case (overnight storage)

The case should be emptied every night and the stock and cash stored in the 'Core' branch safe.

- When this is done, disarm the case totally by turning the alarm key to Off
- Turn off the proximity transmitter overnight as well.

Please remember: You must charge the case for a minimum of eight hours a week.

To activate the case:

The proximity transmitter will manually activate the case. It has two red buttons and one white button. Activation occurs as shown in the table below:

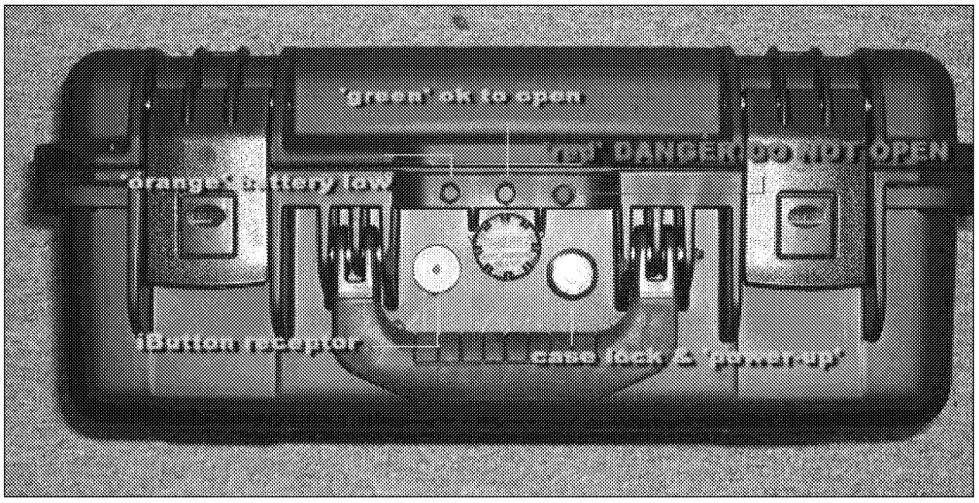
Pressing the white button	will sound the siren intermittently on the case. This can be used as a personal alarm if required.
Pressing the two red buttons	and holding them down for four seconds will fully activate the dye compartment of the case.
Separation from the proximity transmitter	by five metres or more will activate the case if it is in motion
Switching the proximity transmitter off	will activate the case if moved for more than 15 seconds.

Please remember: If the siren goes off while the system is armed, put the case down and do not move it. The case will reset and will not activate.

POL00423229

High Value 'IBIS' security case - instructions for use

The High Value 'IBIS' security case is illustrated below.



Please note: It is strictly forbidden for anyone to operate the case unless they have been fully trained, and have signed and dated the relevant handover document.

Powering the case

An internal battery powers the case. If the orange light shows on the top of the case, the internal battery must be changed within eight hours.

To arm and lock the case

- Unlock and open the case using the ibutton key and flip open the two latches
- Unlock and open the cash compartment using the compartment key
- Place the unwrapped money inside
- Close and lock the cash compartment
- Close the two latches and lock the case lid using the case key
- Place the ibutton onto the receptor and check that the red light in the centre of the receptor lights up for five seconds
- Always keep the keys separate from the case
- Keep the panic transmitter on your person.

Please note: A red flashing light, adjacent to the case lock, means you must not open the case.

To disarm and open the case

- Place the ibutton onto the receptor (a green light will indicate that it is safe to open the case)
- Unlock and open the case using the ibutton key and flip open the two latches
- Unlock and open the cash compartment using the compartment key.

Overnight storage of the empty case

The case should be emptied every night and the stock and cash stored in the 'Core' branch safe.

- Ensure that the case is disarmed (ie, the red light is not flashing).

POL00423229

To activate the case:

Remote activation of the case	Hold down both buttons on the panic transmitter for two and a half seconds. The siren will sound for 15 seconds and then the case will activate. The activation can be stopped by holding down both buttons on the panic transmitter.
Automatic activation of the case	The case will automatically activate if it is attacked in any way, eg with a sledgehammer or a blowtorch.

17.9 Perimeter protection

Sub Office branches

Items provided by Post Office Ltd which give protection to the perimeter generally have a 12 month warranty period during which time Post Office Ltd will ensure that any faults are rectified. After this 12 month period the item becomes the property of the subpostmaster who is then responsible for any continuing maintenance that is required.

18 Maintenance of security equipment

Crown Offices and Sub Office branches

Maintenance of safes and associated secure storage

All safes (including all attached security devices such as mechanical time overlocks, time delay locks, electronic time overlocks and time delay compartments), coin cabinets and Edinburgh boxes which have been supplied by Post Office Ltd are owned and maintained by them.

If a fault occurs with any of this equipment, please phone the following contact point as appropriate:

Type and whereabouts of branch	Contact point	Telephone number
Sub Post Office branches	NBSC	GRO
Crown Offices	Property and Facilities Helpdesk	GRO

Please note: You should not contact Suppliers directly unless you are told to do so.

If you are not satisfied with the service you receive from any contractor:

* Please contact the NBSC to report the problem.

Anti-intruder alarm systems, interconnection units, bandit alarms, electric door bolts and maglocks, CCTV systems, 35mm cameras and Smoke and Dye devices

All anti-intruder alarm systems (W77, 26L, 26L4, 26L4 Mk7, Europlex, Alarm 2000 and European Alarm 2000 (EA2K)), interconnection units, bandit alarms, electric door bolts and maglocks, CCTV systems, 35mm cameras and Smoke and Dye devices which have been supplied by Post Office Ltd are owned and maintained by them.

POL00423229

If a fault occurs with any of this equipment, please phone the following contact point as appropriate:

Type of branch	Contact point	Telephone number
Sub Post Office branches	RoMEC	GRO (24 hour line)
Crown Offices	Property and Facilities Helpdesk	GRO

Please note: You should not contact Suppliers directly unless you are told to do so.

If you are not satisfied with the service you receive from any contractor:

- Please contact the NBSC to report the problem.

Anti-bandit screens

Due to the trauma suffered by sub postmasters following burglaries/robberies, Post Office Ltd has agreed to pay for repairs to anti-bandit screens which are damaged as a direct result of these incidents.

With the sole exception of Screen 2000, installed as part of the ISIS project, in which instance Post Office Ltd pays 60% of the cost of repairs and the subpostmaster 40%, the responsibility for making payment for damage due to all other types of incident rests with the subpostmaster.

Door locks, nuts and bolts, doorstops, springs and glass must be replaced when worn or broken. Replacement components are issued free to sub postmasters with the exception of parcel hatches, doors and doorposts.

The four corner bolts on the parcel hatch must be checked and tightened regularly as this will reduce the problems of broken sash springs and increase resistance in an attack.

If a fault occurs with your anti-bandit screen, please phone the following contact point as appropriate:

Type of branch	Contact point	Telephone number
Sub Post Office branches	NBSC	GRO
Crown Offices	Property and Facilities Helpdesk	GRO

Please note: You should not contact Suppliers directly unless you are told to do so.

If you are not satisfied with the service you receive from any contractor:

- Please contact the NBSC to report the problem.

19 Adjusting your time controlled safe equipment, etc when the clocks go back and forwards

Change from Greenwich Mean Time (GMT) to British Summer Time (BST)

All branches as appropriate

In late March each year when the clocks go forward one hour to allow for the change from Greenwich Mean Time to British Summer Time, you must adjust your security equipment appropriately, as follows:

Mechanical time overlock

When you set the overlock at the close of business on the Saturday when the clocks go forward (or on the Friday if you are not open on the Saturday):

- Deduct one hour from the normal setting time.

POL00423229

Electronic time overlock (ETOL) Mark 5

A set of lights on the outer door of the safe (known as traffic lights) control access to the safe.

At any time between the Monday prior to when the clocks go forward to the Saturday when they actually do:

- Press the BST changeover button (located on the operating panel inside the safe door).

The ETOL will beep to confirm the action.

If it does not beep:

- Press the button again (it will record only once).

The clock will then automatically change to BST on the Sunday.

Electronic time overlock (ETOL) Mark 6

A digital display on the outer door of the safe gives instructions for access.

The following prompt message will be displayed throughout March:

'SUMMER CHANGE MONTH-OK THIS SUNDAY?'

- Ignore this prompt until the Monday prior to the Saturday when the clocks go forward

At any time between the Monday prior to when the clocks go forward to the Saturday when they actually do:

- Press the SUM/WIN button (located on the control panel on the inside door of the safe).

A light will come on to confirm the action.

The clock will then automatically change to BST on the Sunday.

Please note: If you press the SUM/WIN button for too long, the light will come on and go out again, and the changeover will not happen. Please ensure that the light remains on following activation of the button. If the light does go out in the week prior to the clocks going back, you will need to repeat the process.

Matrix Multi Gard unit known as 'La Gard'

The unit is located on the outer door of the safe.

You do not have to take any action as the unit is programmed to change from GMT to BST automatically.

Time controlled burglar alarms (26L)

When you set the alarm at the close of business on the Saturday when the clocks go forward:

- Alter the setting using the 'B' key to turn the switch on the inside face of the limpet plate.

Europlex alarms

- Please refer to your operating instructions booklet or handbook for full instructions

You need to set the clock change between the Monday prior to when the clocks go forward to the Saturday when they actually do. If you fail to do this before the Sunday that follows, a Romec engineer will need to do it.

The basic process is:

- Enter the code
- Press the Shift key

The display will show 'Enter code'

- Do not enter your code a second time
- Press the HELP key.

The display will now show 'Hour Change Sunday'.

The clock will then change at 0200 hours on the Sunday.

POL00423229

Other types of alarms (including European Alarm 2000 (EA2K))

If you have any other type of alarm which displays the time:

- Please consult your user handbook.

Sub Office branches

Sub Office alarms TS690, TS700 and TS900

You must adjust the alarm time display to BST at the close of business on the Saturday when the clocks go forward.

- Please refer to your user manual for full instructions.

The basic process is:

- Enter the code
- Press ENT twice
- Press 2
- Enter the new time using the 24 hour clock
- Press ENT
- Press ESC twice.

Branches with security cameras

It is important that the time shown on all clocks in view of a camera is correct.

- Manually adjust the clock before opening on the first day of business after the time change (refer to the clock instruction manual).
- After you have adjusted the time, please ensure that the clock is replaced securely on its fixings.

Branches with security video equipment

- Manually adjust the digital clock before opening on the first day of business after the time change.

Change from British Summer Time (BST) to Greenwich Mean Time (GMT)

In late October each year when the clocks go back one hour to allow for the change from British Summer Time to Greenwich Mean Time:

- Adjust your particular security equipment in the same way as you did for the change to British Summer Time in March (see above), but add an extra hour to your calculations, rather than deducting it.

POL00423229

20 General information

Remittance procedures may vary slightly across the network according to location and type of branch (for example, some Crown Offices may have premises that can allow the Cash In Transit (CvIT) vehicle to fully enter before delivery or collection takes place.

If 'site-specific 'instructions have been drawn up for your branch, you must adhere to those. The information in this subsection is not intended to be a replacement in these circumstances.

In general, however, the main differences between the procedures for the collection and delivery of Remittances in Post Office branches lie in the level of access to the premises that is allowed to the CvIT staff when they call to make a delivery or collection.

For this reason, you should use this subsection to identify the features of a Remittance transaction that are the same, no matter what type of branch you are (eg, the security or checking of Remittance pouches); instructions apply to all branches unless otherwise indicated.

For information on the transfer of Remittance pouches or the 'Smoke and dye' case to or from the CvIT staff, according to the type of premises you occupy, please see subsection 21; page 72.

20.1 General instructions for the admittance of CvIT staff into your branch

All branches

Because of the security issues involved, CvIT delivery/collection officers must always be treated as the next customer and dealt with immediately. They must take the normal customer route into your branch, whether collecting or delivering. Any exceptions to this practice must be agreed in writing between the Branch or Agency Manager, or sub postmaster, and Network Support Services.

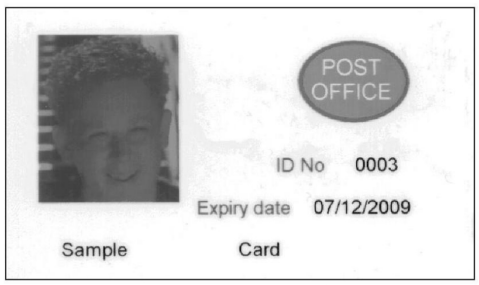
Remittances must not be delivered or collected outside of normal Post Office hours of business (ie, before the secure area opens or closes), or during closure at lunchtime, if applicable.

Identifying the Cash in Transit (CvIT) staff

The identification of the CvIT delivery/collection officers must be fully established before any collection or delivery takes place.

- Always check that the officer is:

- wearing the current uniform
- bearing the current photographic identification pass with serial number as shown below
- carrying a 'Open tag', and their Authorised Collectors' Card (ACC) which is also illustrated below



POL00423229

Preliminary security checks and re-entry to the premises

The Delivery Officer will enter the branch, carry out their normal security checks and hand over the 'Open tag' to the Receiving Officer. The Delivery Officer will then return to the security vehicle to collect the 'Smoke and dye' case.

What happens next depends on whether the CvIT staff are admitted to the secure area of your branch, or whether the transfer of the Remittance pouches from the 'Smoke and dye' case (or in some branches, the case itself) takes place in between the security siphon doors or through a cash/remittance acceptance unit at the counter (see below).

When to admit Cash in Transit (CvIT) delivery and collection officers to the secure area

All branches

CvIT delivery and collection officers must not be admitted into the secure area of the branch unless this has been agreed in writing beforehand between the sub postmaster/ Manager of the branch, and the appropriate parties in Network Support Services.

The secure area is the non-public area within the branch, to which access is restricted and controlled by Post Office staff by electrical or mechanical means, such as the following:

Security siphon doors	Electronic two door siphon entry system where access is controlled by staff within the secure area behind the counter
External Cash Transfer Unit	Metal rotating hatch built into the **external** walls of the premises specifically for the transference of cash, etc.
Internal Cash Transfer Unit	Metal rotating hatch built into the **internal** walls of the premises specifically for the transference of cash, etc

Once the Remittance (or the 'Smoke and dye' case in selected branches) has been passed to you by the CvIT officer, the cash/remittance acceptance unit must be closed immediately.

Branches with a cash/remittance acceptance unit

Remittances must always be accepted or collected via the cash/remittance acceptance unit, unless an alternative such as a two door siphon entry system is provided (see below). The CvIT staff should remain outside the secure area.

Branches without a cash/remittance acceptance unit

In branches where Remittance collections and deliveries cannot be made via a cash/remittance acceptance unit, the CvIT staff may be admitted into the area between the two security siphon doors where the transfer of the Remittance pouches can take place.

Branches with a parcel hatch may accept Remittances through the hatch.

If your branch does not have a cash/remittance acceptance unit, or a two door security siphon door entry system, the CvIT delivery/collection officers may be admitted into the secure area of the branch, though this should always be a last option, and may only be adopted after a careful and thorough identification of the CvIT staff has taken place.

20.2 Security procedure involving the 'Smoke and dye' case

All branches

The 'Smoke and dye' case is the piece of equipment used by the CvIT Delivery Officer for the secure carriage of cash and value items from the security vehicle into the premises where the collection or delivery is to take place.

POL00423229

In most Post Office branches the Delivery Officer delivers the 'Smoke and dye' case to the secure area and transfers the Remittance pouches to the Receiving Officer, but in some branches the 'Smoke and dye' case itself is transferred to the Receiving Officer (see "Case behind the counter' branches' on page 76) so it may be important that you understand how the case works, especially if the alarm should operate accidentally once the case has been taken into the secure area of your branch, or if the 'Smoke and dye' case activates accidentally on the public side of the counter (see below).

The case has a timer which is programmed to count down the amount of time that it takes the Delivery Officer to walk from the security vehicle to the secure area of the premises, and a further amount of time for the return to the security vehicle, after the collection/delivery. The timer in the case only operates while the case is in motion; placing the case on the ground will temporarily stop the timer.

The case is controlled by a Touch Memory Tag, which must be applied to the circular metal disc on the side of the case to change its mode of instruction.

If the case is taken from its intended course, or if it suffers any invasive attack or is subject to any other security violation, it is designed to release 'Smoke and dye', to spoil the cash and render the notes useless to the criminal.

Opening and closing the 'Smoke and dye' case

The 'Smoke and dye' case is opened by applying the 'Open tag' to the circular metal disc on the side.

The three indicator lights on the case will then illuminate as the application of the tag is accepted, and the case will unlock. At this point a single bleep will sound to indicate that the case may be opened.

Please note: If the case is not opened within a few seconds of the bleep sounding, it resets itself. You must in this instance give the case back to the Delivery Officer as they must return to the security vehicle with it.

When a 'Smoke and dye' case is closed after any Remittance pouch to be despatched has been placed inside, the case will lock automatically.

What you should do if the 'Smoke and dye' case goes into alarm in the secure area

If the 'Smoke and dye' case goes into alarm when you have accepted it from the Delivery Officer and it is behind the counter, you will be able to hear the full alarm going off from inside the case.

- Do not panic
- Place the case securely on a level surface
- Do not move the case
- Ask the Delivery Officer for the 'Extend tag'
- Apply the 'Extend tag' to the circular metal disc on the case (the alarm will be silenced and the amount of time for which the case has been programmed will be increased)
- Continue the Remittance transaction as normal.

The following are useful things to remember when you are accepting a 'Smoke and dye' case from a Delivery Officer:

Do not:
• attempt to re-open the case once the lid is closed or partially closed
• stuff the case with oversized packages
• try to force open the lock
• move the case if the alarm is sounding

POL00423229

Do:
• lay the case motionless on the ground if the alarm sounds
• use the 'Extend tag' if the alarm sounds
• apply the tag to the 'Smoke and dye' case for at least 2-3 seconds to ensure that the tag is read

What you should do if the 'Smoke and dye' case activates accidentally in a Post Office branch

If the 'Smoke and dye' case activates accidentally in a Post Office branch, the Delivery Officer must contact their Service Delivery Manager immediately to inform them of the incident.

The Service Delivery Manager will visit the premises within 24 hours to assess the damage, if any.

Effects of the incident on individuals

Following the accidental activation of the equipment, you should assess whether anyone has suffered any ill effects.

No adverse effect is usually associated with contact with coloured smoke. However, it is recommended that persons that have been exposed to it to any substantial degree should evacuate to an open space to reduce the effect of any possible deprivation of oxygen.

No medical or First Aid is likely to be necessary for anyone whose skin has come into contact with the dye, for although the dye may discolour the skin, it can be washed off with soap and water.

If any smoke or dye enters people's eyes, the eyes should be washed with running water for ten minutes. This should be done immediately and if irritation persists, a doctor should be consulted.

Compensation for any damage to premises

Network Support Services employs a team of Loss Adjusters from an insurance company to deal with the financial repercussions of any accidental activation of the 'Smoke and dye' case that may occur within a Post Office branch.

If the cost of repairing the damage to the branch involved is agreed to be less than £250, Network Support Services will pay the owners of the branch directly by cheque, provided receipts for repairs are provided.

If the cost of repairs to the property are expected to come to more than £250, the owners must complete a claim form supplied by the Service Delivery Manager. The Service Delivery Manager contacts Network Support Services in Manchester, who in turn advise the Loss Adjusters of the claim. Within 48 hours of the claim form being supplied to the Post Office branch, the Loss Adjusters will arrange a meeting with the owners of the branch to collect the completed claim form and to provide information on how the claim will be processed.

20.3 Securing Remittances

All branches

Please note: The following procedures for the security of Remittances will apply to all branches unless a separate procedure has been agreed in writing for your branch.

When the Receiving Officer has scanned all of the banknote pouches, etc, they must store them in the main safe as soon as possible.

Remittances must never be left on the counter top, or any other work top (including cupboards), whether in view of the general public or not, for even the shortest period of time.

Delivery of Remittances

Please note: The Delivery Officer must make more than one trip to the security vehicle when delivering Remittance pouches if the combined values of the pouches exceeds £25,000.

POL00423229

Branches with an Edinburgh box

At branches where two banknote pouches are delivered as routine, an Edinburgh box will normally be installed as standard procedure.

If you have an Edinburgh box in your branch (see 'Edinburgh Boxes' on page 42), this must be left open when a Remittance delivery is expected, and the keys secured in a 'time delay' locked safe. The box must be used for the immediate acceptance and temporary retention of banknotes.

The banknotes must be placed in the Edinburgh box immediately after removal from the CvIT equipment, and the lid of the box closed. Banknotes must then be transferred to the main safe the next time it is opened. The main safe need not be opened specifically to transfer the banknotes to the safe.

Branches without an Edinburgh box

If your branch does not have an Edinburgh box and your Post Office safe does not have a **four minute** time delay lock, you must place the Remittance in the safe as soon as it has been delivered, before you begin serving customers again.

If your branch does not have an Edinburgh box and your Post Office safe has a time delay lock, you must turn the safe key as soon as the CvIT Delivery Officer arrives at your branch, so that the time delay releases as soon as possible, and you can safely transfer the contents of the Remittance to the main safe.

If your branch has a second safe without a time delay lock, or a lockable cupboard or drawer, the Remittance must be stored in this, with the key withdrawn, until the time delay on the main safe releases.

Branches without a Horizon terminal in the secure area

There are specific instructions relating to the immediate securing of the contents of Remittance deliveries in branches that do not have a Horizon terminal in the secure area, so that Remittance pouches can be scanned into the Horizon system as pouches are transferred from the Delivery Officer to the Receiving Officer (see 'Branches that do not have a Horizon terminal in the secure area' on page 74).

Collection of Remittances

Remittances that are due for collection must be kept in the main safe (a four minute 'time delay' lock safe if one is fitted), until the CvIT delivery officer arrives at your branch to collect them.

The correct CvIT process is that upon being notified of the four minute time delay lock, the CvIT crew must return to their vehicle to enable the time period to elapse, after which time they will check everything is okay and make the collection.

If you should experience problems with CvIT crews refusing to wait for the safe to unlock please contact the NBSC on 0845 601 1022 selecting option 3 to report the incident.

If coin is included in the Remittance, it may be left on the floor of the secure area, out of sight of the general public, if no more suitable secure accommodation (ie,a second safe or coin container) is available when a Remittance collection is expected. Care must be taken to ensure that any coin, left ready for collection in this manner, does not constitute a safety hazard (ie, staff will not trip over coin bags).

More than one pouch

If two banknote pouches or more are being despatched from your branch, both may be removed from the time delay locked safe once the Delivery Officer has arrived at your branch. The safe door must be closed and locked immediately the Remittance pouches have been removed. The second pouch must be placed temporarily in the second safe or coin container in the branch, where applicable, while the Delivery Officer transfers the first pouch to the secure vehicle.

If no second safe or coin container has been fitted in your branch, the second pouch must be left in the time delay locked safe, with the door closed and the time delay lock released and counting down. Under no circumstances should the safe door be left open or the Remittance pouch left on the floor of the secure area until the Delivery Officer returns.

Please note: The Delivery Officer must make more than one trip to the security vehicle with the Remittance pouches if the combined values of the pouches exceeds £25,000.

POL00423229

Branches in Northern Ireland

Remittances that are due for collection must be kept in the main safe (a fifteen minute 'time delay' lock safe if one is fitted. The time delay lock may be activated about fifteen minutes before the CvIT delivery officer is expected to arrive. If the CvIT crew is running late, they should inform you.

20.4 Checking Remittances

All branches

Remittance pouches and coin bags must always be scanned as soon as they are delivered to your branch; for full instructions, see Cash and Secure Stock Remittance services booklet; Automated Remittances; Remittances In (cash).

However, you must leave Remittances in the main safe or Edinburgh box for at least 30 minutes before checking the contents, unless there is an urgent operational need to remove and count any of the cash.

Please remember: Most robberies involving Remittances occur within 30 minutes of the Remittance being delivered.

When it is safe to check the Remittance, the number of packets of cash must be counted to ensure that the total value of the Remittance agrees with that printed on the Remittance advice accompanying the pouches, before the packets are re-secured in the main safe.

The contents of individual Plastic Banknote Envelopes should be checked when the cash is required at the counter to prevent the removal of too much cash from secure storage in one go, bearing in mind that any discrepancies in banknote envelopes must be reported to the Cash Centre helpline within 48 hours of receipt.(see Methods of Payment booklet; Cash handling; General information).

21 Delivery and collection procedures relating to specific types of branch

In all of the instructions in this subsection the term 'Receiving Officer' relates to the Branch Manager, the sub postmaster, etc, or any staff members who are authorised to accept or despatch Remittances at branches; 'Delivery Officer' refers in each case to the Cash in Transit (CvIT) delivery or collection officer.

Please note: Screen-less branches are issued with specific instructions relating to Remittance delivery and collection when they are fitted out. Instructions may vary according to types of screen-less branch and must be rigorously applied.

All branches with a cash/remittance acceptance unit (not Crown Offices)

Please note: These instructions apply to branches with a cash/remittance acceptance unit, whether screened or screen-less.

If you have a cash/remittance acceptance unit in your branch which is suitable for the acceptance of a 'Smoke and dye' case, all Remittance collections and deliveries must take place through the unit and the CvIT Delivery Officers **must not** be admitted into the secure area of the branch.

Any exceptions to this process must be agreed in writing between the manager or sub postmaster of the branch, and the appropriate parties in Network Support Services.

Please note: The only alternative method of transferring the Remittance that may be used in this type of branch is when the branch has an electronic two door siphon entry system, in which case the physical transfer of the Remittance may take place between the siphon doors (see 'Crown Offices only' on page 75).

Delivery of Remittances

The identification of the CvIT delivery/collection officers must be fully established before any collection or delivery takes place (see 'Identifying the Cash in Transit (CvIT) staff' on page 67).

POL00423229

The Delivery Officer will enter the branch, carry out their normal security checks and hand over the 'Open tag' to the Receiving Officer who remains in the secure area of the branch. The Delivery Officer will then return to the security vehicle to collect the 'Smoke and dye' case.

Please remember: At this point the time delay lock on the main safe must have been released, in order that the Remittance may be secured as soon as possible.

The Delivery Officer will re-enter the branch with the 'Smoke and dye' case, and approach the cash/remittance acceptance unit to reclaim the 'Open tag' from the Receiving Officer. They will then apply the tag to the circular metal disc on the case in order to transfer the Remittance pouch to the Receiving Officer via the cash/remittance acceptance unit.

Please note: If coin forms part of the Remittance being delivered, this should be handed over first, before the banknotes. The Delivery Officer can deliver the coin into the branch when they first enter to announce their arrival and to deliver the 'Open tag'.
The Receiving Officer can leave the coin bags on the floor of the secure area until the banknote pouches have been transferred, and while the main safe delay lock is being released.

Once the Remittance pouch has been handed to the Receiving Officer by the Delivery Officer, the unit must be closed immediately.

Please note: If the cash/remittance acceptance unit used is a parcel hatch, the hatch must not be opened any wider than is absolutely necessary in order to allow the Remittance pouch to be handed over to the Receiving Officer. The parcel hatch must be secured immediately the case has been passed through

Depending on whether the combined value of the Remittance pouches to be delivered exceeds £25,000, the Delivery Officer may need to make more than one trip to transfer the pouches from the secure vehicle. Each Remittance pouch delivered must be passed through the parcel or cash/remittance acceptance unit in the same way. The 'Open tag' must be kept by the Receiving Officer on the secure side of the counter and passed across to the Delivery Officer each time they are ready to transfer a pouch from the 'Smoke and dye' case. It must not be given back until the last Remittance pouch has been safely transferred.

Please note: The main safe must not be left open to receive the contents of the pouches while the Delivery Officer returns to their security vehicle to collect each successive pouch.

The Receiving Officer must check each pouch against the Pouch Delivery receipt, and when the final pouch has been transferred, they must scan the receipt on the Horizon system before the Delivery Officer leaves the premises.

When the Receiving Officer has scanned all of the Remittance pouches, they must secure the banknotes in the main safe as soon as possible; for full information on the security of Remittances, see para 20.3; page 70.

Collection of Remittances

For information on the security of Remittances that are being despatched from a branch, see para 20.3; page 70.

In the case of a Remittance collection, the Delivery Officer must present their Authorised Collectors' Card for scanning before the Receiving Officer transfers any pouches.

Remittance pouches for despatch must be passed to the Delivery Officer through the cash/remittance acceptance unit in the same way as the Remittances pouches that are delivered.

Please remember: All Remittance pouches to be despatched must be scanned out on the Horizon system before they are transferred to the Delivery Officer and placed in the 'Smoke and dye' case.

Depending on whether the combined value of the Remittance pouches to be despatched exceeds £25,000, the Delivery Officer may need to make more than one trip to transfer the pouches to the secure vehicle. The 'Open tag' must remain in the possession of the Receiving Officer until the last pouch is transferred, and only passed across to the Delivery Officer when they are ready to place a pouch in the 'Smoke and dye' case for transfer to their secure vehicle.

When the last Remittance pouch for despatch is placed in the 'Smoke and dye' case, the 'Open tag' must be returned to the Delivery Officer, who should lock it inside the case with the final pouch, before they return the case to the secure vehicle.

POL00423229

When a Remittance collection is combined with a delivery

If the Delivery Officer is collecting Remittance pouches that are ready for despatch, as well as making a delivery, the Receiving Officer can begin to transfer the outgoing pouches to the Delivery Officer as soon they receive the first Remittance pouch (as long as the Authorised Collectors' Card has been scanned) so that the trips that the Delivery Officer needs to make to their secure vehicle are kept to a minimum.

Screen-less branches without a cash/remittance acceptance unit

If you do not have a cash/remittance acceptance unit in your branch, CvIT Delivery Officers must be admitted into the secure area of the branch to collect and deliver Remittances.

Delivery of Remittances

The identification of the CvIT delivery/collection officers must be fully established before any collection or delivery takes place (see 'Identifying the Cash in Transit (CvIT) staff' on page 67).

The Delivery Officer will enter the branch, carry out their normal security checks and hand over the 'Open tag' to the Receiving Officer who remains in the secure area of the branch. The Delivery Officer will then return to the security vehicle to collect the 'Smoke and dye' case.

Please remember: At this point the safe time delay should be timing down and when released the Remittance should be placed in the safe as soon as possible. The counter access door should not be open when the safe door is open.

When the Delivery Officer re-enters the branch, they must be admitted to the secure area of the branch by the Receiving Officer. Having retrieved the 'Open tag', the Delivery Officer will then open the 'Smoke and dye' case by applying the tag to the circular metal disc on the case. The Delivery Officer will remove the contents and hand them to the Receiving Officer.

Please note: If coin forms part of the Remittance being delivered, this should be handed over first, before the banknotes. The Delivery Officer can deliver the coin into the branch when they first enter to announce their arrival and to deliver the 'Open tag'.
The Receiving Officer can leave the coin bags on the floor of the secure area until the banknote pouches have been transferred, and while the main safe delay lock is being released.

Depending on whether the combined value of the Remittance pouches to be delivered exceeds £25,000, the Delivery Officer may need to make more than one trip to the secure vehicle in order to deliver all of the pouches. The 'open tag' must remain in the secure area of the branch until all the pouches have been transferred to the Receiving Officer.

Please note: The main safe should not be left open to secure all of the pouches if the Delivery Officer has to make repeated trips to the secure vehicle to collect all of the pouches that need to be delivered.

When the last Remittance pouch has been safely delivered, the 'Open tag' must be returned to the Delivery Officer, who should lock it inside the case with the final pouch, before they return the case to the secure vehicle.

The Receiving Officer must check the pouches against the Pouch Delivery receipt, and scan the receipt on the Horizon system. How this is achieved is dependant on whether there is a Horizon terminal in the secure area of the branch.

Branches that have a Horizon terminal in the secure area

The Receiving Officer must check each pouch against the Pouch Delivery receipt, and when the final pouch has been transferred, they must scan the receipt on the Horizon system before the Delivery Officer leaves the premises.

When the Receiving Officer has scanned all of the Remittance pouches, they must secure the banknotes in the main safe as soon as possible; for full information on the security of Remittances, see para 20.3; page 70.

Branches that do not have a Horizon terminal in the secure area

As soon as each pouch is taken from the 'Smoke and dye' case, the Receiving Officer must remove the banknote envelopes from the Remittance pouch for immediate secure storage in the main safe.

POL00423229

The Receiving Officer must then scan the empty Remittance pouches into the Horizon system once all banknotes are secure.

Please note: Under no circumstances may full Remittance pouches be scanned into the Horizon system, unless there is a Horizon terminal in the secure area of the branch.

The Receiving Officer and the Delivery Officer **must not** leave the secure area, nor open any doors leading into the secure area, until the banknote envelopes have been secured in the four-minute time delay protected safe or an Edinburgh box, if one is provided.

Collection of Remittances

For information on the security of Remittances that are being despatched from a branch, see para 20.3; page 70.

In the case of a Remittance collection, the Delivery Officer must present their Authorised Collectors' Card for scanning before the Receiving Officer transfers any pouches.

Remittance pouches for despatch must be passed to the Delivery Officer through the cash/remittance acceptance unit in the same way as the Remittances pouches that are delivered.

Please remember: All Remittance pouches to be despatched must be scanned out on the Horizon system before they are transferred to the Delivery Officer and placed in the 'Smoke and dye' case.

Depending on whether the combined value of the Remittance pouches to be despatched exceeds £25,000, the Delivery Officer may need to make more than one trip to transfer the pouches to the secure vehicle. The 'Open tag' must remain in the possession of the Receiving Officer until the last pouch is transferred, and only passed across to the Delivery Officer when they are ready to place a pouch in the 'Smoke and dye' case for transfer to their secure vehicle.

When the last Remittance pouch for despatch is placed in the 'Smoke and dye' case, the 'Open tag' must be returned to the Delivery Officer, who should lock it inside the case with the final pouch, before they return the case to the secure vehicle.

When a Remittance collection is combined with a delivery

If the Delivery Officer is collecting Remittance pouches that are ready for despatch, as well as making a delivery, the Receiving Officer can begin to transfer the outgoing pouches to the Delivery Officer as soon they receive the first Remittance pouch (as long as the Authorised Collectors' Card has been scanned) so that the trips that the Delivery Officer needs to make to their secure vehicle are kept to a minimum.

Crown Offices only

Delivery of Remittances

The identification of the CvIT delivery/collection officers must be fully established before any collection or delivery takes place (see 'Identifying the Cash in Transit (CvIT) staff' on page 67).

After the Delivery Officer has carried out their normal security checks and handed over the 'Open tag' to the Receiving Officer, they will return to the security vehicle to collect the 'Smoke and dye' case.

Please remember: At this point, if applicable, the time delay lock on the main safe must have been released, in order that the Remittance may be secured or transferred as soon as possible (see para 20.3; page 70).

When the Delivery Officer re-enters the branch with the 'Smoke and dye' case, they must be re-admitted to the area between the two doors of the electronic siphon entry system by the Receiving Officer. The Receiving Officer will pass the 'Open tag' to the Delivery Officer when they are inside the security siphon area. The Delivery Officer will then open the 'Smoke and dye' case and remove the contents.

If coin forms part of the Remittance being delivered, this should be handed over first, before the banknotes. The Delivery Officer can deliver the coin into the branch when they first enter to announce their arrival and to deliver the 'Open tag'. The Receiving Officer can leave the coin bags on the floor of the secure area until the banknote pouches have been transferred, and while the main safe delay lock is being released.

POL00423229

Depending on whether the combined value of the Remittance pouches to be delivered exceeds £25,000, the Delivery Officer may need to make more than one trip to transfer the pouches from the secure vehicle. The 'Open tag' must remain in the possession of the Receiving Officer until the last pouch is delivered. The main safe must not be left open to receive the contents of each pouch while the Delivery Officer returns to their security vehicle to collect each successive pouch.

After each transfer of a Remittance pouch inbetween the siphon doors, the Receiving Officer must check it against the Pouch Delivery receipt, before taking it into the secure area with the 'Open tag'. The Delivery Officer is not given access to the secure area.

Until the Remittance transfer is completed, (ie, all the pouches have been transferred to the secure area), the Delivery Officer must remain within the electronic siphon entry system. Before the Delivery Officer leaves this area, the Receiving Officer must scan the receipt on the Horizon system.

The Receiving Officer must then scan all of the pouches that have been delivered on the Horizon system, after which the pouches must be secured in the main safe as soon as possible.

Please note: The Receiving Officer must not leave the secure area of the branch, or open the door to the secure area, under any circumstances, until the contents of the Remittance have been secured in the main safe or the Edinburgh box.

Collection of Remittances

For full instructions relating to the security of pouches or coin bags to be despatched, see para 20.3; page 71.

In the case of a Remittance collection, the Delivery Officer must present their Authorised Collectors' Card for scanning before the Receiving Officer transfers any pouches.

Remittance pouches for despatch must be passed to the Delivery Officer inbetween the siphon doors with the 'Open tag'. Each pouch must be placed in the 'Smoke and dye' case, prior to transfer to the security vehicle.

Please remember: All Remittance pouches to be despatched must be scanned out on the Horizon system before they are transferred to the Delivery Officer and placed in the 'Smoke and dye' case.

Depending on whether the combined value of the Remittance pouches to be despatched exceeds £25,000, the Delivery Officer may need to make more than one trip to transfer the pouches to the secure vehicle. The 'Open tag' must remain in the possession of the Receiving Officer until the last pouch is transferred

The electronic siphon entry system must be secured immediately the Delivery Officer has left the secure area on each trip they make to the secure vehicle with Remittance pouches.

When the last Remittance pouch for despatch is placed in the 'Smoke and dye' case, the 'Open tag' must be returned to the Delivery Officer, who should lock it inside the case with the final pouch, before they return the case to the secure vehicle.

When a Remittance collection is combined with a delivery

If the Delivery Officer is collecting Remittance pouches that are ready for despatch, as well as making a delivery, the Receiving Officer can begin to transfer the outgoing pouches to the Delivery Officer as soon they receive the first Remittance pouch (as long as the Authorised Collectors' Card has been scanned) so that the trips that the Delivery Officer needs to make to their secure vehicle are kept to a minimum.

'Case behind the counter' branches

In branches where the attempted robbery of Remittance pouches being transferred at the counter has become more frequent, a policy has been implemented where the Receiving Officer accepts the 'Smoke and dye' case (rather than the individual cash pouches) from the Delivery Officer via the cash/remittance acceptance unit, and removes the contents away from the counter where there is increased security.

Apart from the fact that the Receiving Officer opens and empties the case, and places inside any Remittances for despatch for transfer to the secure vehicle, rather than the Delivery Officer, the other aspects of the Remittance delivery and/or collection remain the same.

POL00423229

Delivery of Remittances

The identification of the CviT delivery/collection officers must be fully established before any collection or delivery takes place (see 'Identifying the Cash in Transit (CviT) staff' on page 67).

The Delivery Officer will enter the branch, carry out their normal security checks and hand over the 'Open tag' to the Receiving Officer who remains in the secure area of the branch. The Delivery Officer will then return to the security vehicle to collect the 'Smoke and dye' case. At this point the time delay lock on the main safe must have been released, in order that the Remittance may be secured as soon as possible.

Please note: If coin forms part of the Remittance being delivered, this should be handed over first, before the banknotes. The Delivery Officer can deliver the coin into the branch when they first enter to announce their arrival and to deliver the 'Open tag'.
The Receiving Officer can leave the coin bags on the floor of the secure area until the banknote pouches have been transferred, and while the main safe delay lock is being released.

The Delivery Officer will re-enter the branch with the 'Smoke and dye' case, and transfer it to the Receiving Officer via the cash/remittance acceptance unit. Once the Remittance or 'Smoke and dye' case has been handed to the Receiving Officer by the Delivery Officer, the unit must be closed immediately.

Please note: If the acceptance unit used is a parcel hatch, the hatch must not be opened any wider than is absolutely necessary in order to allow the 'Smoke and dye' case to be handed over to the Receiving Officer. The parcel hatch must be secured immediately the case has been passed through.

In a secure area away from the counter the Receiving Officer must apply the 'Open tag' to the circular metal disc on the side of the 'Smoke and dye' case in order to open it (see para 20.2; page 69) before removing the contents and checking them against the delivery note.

Depending on whether the combined value of the Remittance pouches to be delivered exceeds £25,000, the Delivery Officer may need to make more than one trip to transfer the pouches from the secure vehicle. In each instance the 'Smoke and dye' case must be transferred to the Receiving Officer with the 'Open' tag via the cash/remittance acceptance unit in the same way as the initial delivery. The 'Open tag' must be kept by the Receiving Officer on the secure side of the counter while the 'Smoke and dye' case is emptied of each pouch, until the last Remittance pouch has been transferred.

Please note: The main safe must not be left open to receive the contents of the pouches while the Delivery Officer returns to their security vehicle to collect each successive pouch.

The Receiving Officer must check each pouch delivered against the Pouch Delivery receipt, and when the final pouch has been transferred safely, they must scan the receipt on the Horizon system before the Delivery Officer leaves the premises.

When the Receiving Officer returns the 'Smoke and dye' case to the Delivery Officer after the last pouch has been transferred, they must first place the 'Open tag' inside the case.

After the Receiving Officer has scanned all of the Remittance pouches, etc, they must secure the banknotes in the main safe as soon as possible; for full information on the security of Remittances, see para 20.3; page 70.

Coin delivery

If coin forms part of the Remittance being delivered, this should be handed over first, before the banknotes. The Delivery Officer can deliver the coin into the branch when they first enter to announce their arrival and to deliver the 'Open tag'. The Receiving Officer can leave the coin bags on the floor of the secure area until the banknote pouches have been transferred, and while the main safe delay lock is being released.

Collection of Remittances

For information on the security of Remittances that are being despatched from a branch, see para 20.3; page 70.

In the case of a Remittance collection, the Delivery Officer must present their Authorised Collectors' Card for scanning before the Receiving Officer transfers any pouches.

Remittance pouches for despatch must be placed in the 'Smoke and dye' case by the Receiving Officer in a secure place away from the counter in the same way as the delivery pouches that are removed from the case (see 'Delivery of Remittances' above).

POL00423229

Each time a Remittance pouch for despatch has been secured in the 'Smoke and dye' case, the Receiving Officer must close the case and return the case to the Delivery Officer via the cash/remittance acceptance unit. The 'Open tag' must remain with the Receiving Officer until the final transfer takes place.

Please note: If the acceptance unit used is a parcel hatch, the hatch must not be opened any wider than is absolutely necessary in order to allow the 'Smoke and dye' case to be handed over to the Delivery Officer. The parcel hatch must be secured immediately the case has been passed through.

The final Remittance pouch that is to be collected from the Receiving Officer is placed in the 'Smoke and dye' case, along with the 'Open tag'. The case must then be returned to the Delivery Officer through the cash/remittance acceptance unit as normal.

When a Remittance collection is combined with a delivery

If the Delivery Officer is collecting Remittance pouches that you are despatching, as well as making a delivery, the Receiving Officer can begin by placing the first Remittance pouch for collection in the 'Smoke and dye' case as soon as they have removed the first delivery pouch (as long as the Authorised Collectors' Card has been scanned), before they return the case and the 'Open tag' to the Delivery Officer. In this way the trips that the Delivery Officer needs to make to their secure vehicle are kept to a minimum.

Rural screen-less format branches

Despatch and collection of Remittances

All Remittances must be collected and delivered using the normal customer route into the premises, but the branch must be closed to customers before the 'Smoke and dye' case is delivered into the branch. Any exceptions to this instruction must be agreed in writing between the manager or sub postmaster of the branch, and the appropriate parties in Network Support Services.

The identification of the CviT delivery/collection officers must be fully established before any collection or delivery takes place (see 'Identifying the Cash in Transit (CviT) staff' on page 67).

Please remember: At this point, if applicable, the time delay lock on the main safe must have been released, in order that the Remittance may be secured or transferred as soon as possible.

After the Delivery Officer has carried out their normal security checks and handed over the 'Open tag' to the Receiving Officer, they will return to their security vehicle to collect the 'Smoke and dye' case. Re-entry to the branch will only take place as soon as the premises are clear of customers and the external doors have been closed.

One the premises are clear of customers, the branch must be closed, and all external doors locked for the duration of the Remittance collection/delivery. Once the external doors have been locked, the Receiving Officer must remain at the main door of the premises, ready to re-admit the Delivery Officer to the branch with the case and the 'Extend tag'.

Depending on whether the combined value of any Remittance pouches being delivered or collected exceeds £25,000, the Delivery Officer may need to make more than one trip to transfer the pouches to or from the secure vehicle. In each instance the Delivery Officer must return the 'Smoke and dye' case to the secure vehicle while the Receiving Officer remains at the external door of the premises, until the last Remittance pouch has been transferred.

Please note: The main safe must not be left open to receive the contents of the pouches while the Delivery Officer returns to their security vehicle to collect each successive pouch.

Coin delivery

If coin forms part of the Remittance being delivered, this should be handed over first, before the banknotes. The Delivery Officer can deliver the coin into the branch when they first enter to announce their arrival and to deliver the 'Open tag'. The Receiving Officer can leave the coin bags in a secure place while the main safe delay lock is being released.

POL00423229

When a Remittance collection is combined with a delivery

If the Delivery Officer is collecting Remittance pouches that are ready for despatch, as well as making a delivery, the Receiving Officer can begin to transfer the outgoing pouches to the Delivery Officer as soon they receive the first Remittance pouch (as long as the Authorised Collectors' Card has been scanned) so that the trips that the Delivery Officer needs to make to their secure vehicle are kept to a minimum.

Securing Remittances

Remittances being delivered

Once the Remittance pouch has been transferred from the Delivery Officer and scanned into the Horizon system, it must immediately be deposited into the Drop Drawer Deposit Safe until it can be checked.

Remittances being collected

Any Remittances to be despatched must be kept secure in the Drop Drawer Deposit Safe until the Delivery Officer arrives at your branch.

POL00423229

22 Personal security for everyone

This subsection deals with personal security outside the workplace.

Please note: As each individual's personal circumstances are different, the instructions included here are intended as advice only, based on best practice adopted in general situations. They are not mandatory but are wholly endorsed both by Post Office Ltd and the National Federation of Sub Postmasters, and you are strongly advised to follow the recommendations for the different scenarios which are covered and apply common sense in order to effectively protect yourself and your family by attempting to prevent potentially dangerous situations from threatening your domestic circumstances.

There are many practical things you can think about and do to reduce the risk of anything happening to you or members of your family by taking sensible precautions. You may be aware of some of the suggestions already but some may be new to you and you may find them useful.

The best defence is to develop an awareness of the times when you are most at risk.

Learn to recognise vulnerable situations so that you can avoid them whenever possible

Vulnerability means openness to an attack. Strict routines create criminal opportunities.

- Consider the following:

When am I most vulnerable to attack?
When is my family most at risk?
Am I careful to maintain personal security when I answer the door at home?
Do I take the time to watch what is happening around me as I prepare to drive off in my car?
Are my movements so predictable that they put me at risk from a possible assailant?
Do I need to consider altering my routine so that it does not put me at risk?

You never know when you are being watched. You will not wish to alarm your family or cause them any undue distress, but the unfortunate reality is that a threat to your welfare may exist and you should always remain vigilant. You should try to reduce the occasions when you are most vulnerable to attack and vary your routine so that anyone who may be watching finds it hard to predict your movements.

Always be alert, always be prepared for possible attack

When an attacker looks at you and your family as a potential target he will be discouraged if he sees you are on your guard; then he will look elsewhere for an easier target.

When you take sensible precautions for your personal security:

- Make sure your family does too
- Never forget that any member of your family could be targeted.

When you have finished work:

- Remove all forms of identification that say who you are or what work you do
- Beware of bogus telephone calls from persons claiming to be the Police or Post Office Ltd personnel (always verify calls on a number known to you)
- Never reveal things about yourself and your family unless it is essential (idle chatter is part of human nature, but it is something which could be used to criminal advantage)

If you are selling your property:

- Be wary when potential purchasers come to view

POL00423229

- Ensure that they are only shown around the Post Office area when the safes are locked, alarmed and the keys are off-site.

Don't hesitate - call 999

Raising an alarm and acting defensively can often deter a potential attacker from continuing with an attack.

If you feel threatened:

- Always telephone the police.

If you cannot get to a telephone:

- Use your initiative
- Scream and shout if you feel you are coming under attack
- Make as much noise as possible if that is the best way to attract attention other people's attention to your situation
- Consider providing your family with personal alarms that can be used at the first of any trouble.

Think about ways to safeguard your family while at home

To safeguard you and your family in your home, please consider the following precautions:

- Do not let anybody into your home unless you are sure of their identity (insist on seeing and verifying identity for all meter readers, sales people and other unexpected visitors)
- Consider fitting a door chain (always use it while you find out who is calling or while you check for any potential signs of trouble)
- Ensure that you keep track of the whereabouts of all your house keys (if a set of keys goes missing, change the locks); never hide keys under the door mat or plant pots
- Keep exterior doors locked whenever possible
- Never allow young children to answer the door
- Never leave the house in darkness when you go out at night
- If you are going away on holiday and are on good terms with neighbours, ask them to keep an eye on your property
- Always cancel regular deliveries to your door such as milk or newspapers.

Please note: If you have a neighbourhood or home watch scheme in your area, you should consider joining it. The schemes are a good idea for getting people together to help prevent crime and make their neighbourhood a safer place.

POL00423229

- Check the security of your home against the following advice (you will need to judge which of the following recommendations are right for you, your home and your personal circumstances):

Make sure exterior doors are of strong solid core construction (the door structure and frame should be of an equal strength to the locks)
You are advised to fit British standard approved five lever mortice deadlocks to all exterior doors and fit dead bolts into the door frame
Consider seriously fitting a peephole into the front door so that you can see outside before opening, and a door chain to restrict opening the door until you know the identity of the caller
Where you have glass panels, fit blinds to make sure anybody outside cannot see in
Fit window locks to all ground floor windows and to any upstairs windows where there is easy access
If you are getting new glass for windows, consider laminated glass as it is harder to break, or security grilles or small paned Georgian style windows. If you have double glazing, check with the manufacturer to ensure that the glass cannot be removed from the outside.
Light your front door area at night. If you have a concealed garden or backyard, think about fitting lights to illuminate them. Exterior lighting that responds to movement is now widely available. These kind of lights should be positioned out of normal reach and with concealed wiring. If you use ordinary lights that you switch on and of, operation should be from inside the home only.
For patio doors, obtain specialist advice on fitting locks (ideally these doors should have special locks fitted top and bottom unless a multi-locking system is used). Consider installing an anti-lift device to stop a thief simply lifting the door off its rail. Fit security mortice locks to French doors and mortice bolts to the top and bottom of both doors.
If you have a passage at the side of your house, prevent criminals from getting to the back of the house where they can work with less chance of being seen, by fitting a strong high gate across the passage. If you share an alleyway with a neighbour, talk to them about sharing the cost.
Garages and sheds should be kept locked, especially if there is a connecting door to the house (ensure that you lock tools and ladders away so that a thief cannot use them to break in)
Be wary when letting pets out at night into the garden (criminals have been known to enter premises through rear doors when they are left unlocked or when pets have been let in again)
Be wary of shrubs, bushes or sheds near to your home where criminals could hide
Consider investing in a timer to switch on the lights automatically in your home at dusk
Keep a torch or candles to hand to act as reserve emergency lighting should the power be cut off in your home
Consideration should be given to risk of fire and the means of escape, should it become necessary (fit a smoke detector conforming to British standard 5446)

Think about security relating to telephones in your home and anonymous callers

Telephone wires should enter a residential building at the first floor level to prevent tampering. If this is not possible, the wires should be protected by a metal sheath.

- If you do not have a telephone extension near to your bed, consider having one installed (it will make you feel more secure as it allows you to call the Police immediately without alerting an intruder)
- Emphasise to your family that they must not reveal the whereabouts of any family member if a stranger calls (insist that messages are taken properly with a name and number in order that you can call back)

When using a radio telephone (ie hand held portable with an aerial):

- Remember that it is easy for somebody outside to listen in to your conversation from another device.

POL00423229

Anonymous calls are always disturbing and must never be ignored.

- Always take threatening calls seriously and report them to the Police
- Consider also keeping a pad near to your telephone(s) in order to make any notes that may help the Police
- Keep a note of the time and date of the call and what is said
- Keep the caller talking as long as possible (note what the voice sounds like, eg male, female, young or old).
- Try to detect whether the caller has an identifiable regional or foreign accent (write down your thoughts while the person is still talking)
- Try to determine the tone of the caller (eg does the voice sound angry, etc)
- See if you can hear any noise in the background, such as telephones ringing, the noise of machinery, music, or voices, etc
- Call the police as soon as the caller rings off.

If you find yourself disturbed by anonymous callers, there are positive steps that can be taken.

- Always seek Police advice
- Dial 1471 to see if you can obtain the caller's number
- Have your number changed and go 'ex-directory'
- Arrange for an operator to intercept all incoming calls.

Think about ways to stay safe while driving and in your car

Experience shows that journeys alone by car are the times when kidnap targets are most at risk.

- Think about your frequent journeys (whenever possible, vary your route, your time of arrival and time of departure).

Before getting into your car

- Check the tyres for any damage
- Check the back seat and the boot to make sure nobody is lying in wait for you
- Look around the car to check whether there is anything that makes you suspicious
- Find out the whereabouts of Police stations in the general area of work and home
- If you suspect that you are being followed or watched, make a detour to your nearest Police station or another place of safety, and report your concern to the Police
- Keep to well-lit roads when driving
- Avoid parking in the same place each day.

Before you make a long trip:

- Make sure your vehicle is in good condition and you have sufficient oil, water and fuel
- Plan how to get to your destination before you leave and stay on main roads if you can
- Keep a mobile phone, phone card or change handy in case you need to make a telephone call
- Always keep a torch in your car
- Tell anyone you are planning to meet what time you think you will get there and the route you are taking.

While you are driving:

- Keep all doors and windows of the car locked
- Never give lifts to hitchhikers or strangers

POL00423229

- Drive carefully at a steady speed.

Please remember: Adopting a defensive driving attitude does not mean disregarding traffic laws or ignoring the Highway Code.

Impersonation of Police officers is not unknown.

If you are suspicious for any reason when stopped by the Police:

- Ask to see a warrant card before opening the window all the way down or getting out of the car.

23 Robberies and evacuations

All branches

23.1 Reporting of incidents

All robberies, burglaries and any other incidents that arouse your suspicions must always be reported to the Police and the NBSC. You should always give as much information as possible, including reasons why a particular incident has made you suspicious. Even if your branch is not targeted for criminal action, details that you provide may help to prevent an attack on other premises.

Dealing with the media

Under no circumstances should you speak to the media about any security procedures or security equipment in operation in Post Office branches, or discuss any amounts of cash or stock stolen. In addition, no member of staff or sub postmaster may agree to take part in a television reconstruction of an incident without the permission of Post Office Ltd senior management

All media enquiries must be referred to the NBSC.

23.2 Armed robbery

While it is hoped that you will never have to undergo the trauma of an armed robbery, you must be aware of the guidelines to follow both during and after the hold-up. This will assist the Police in their attempts to identify and convict the criminals.

During a hold-up

- If there is a bandit alarm in your branch, activate it only if it is safe to do so
- If there is a security camera in your branch, activate it if it is safe to do so
- Obey instructions given and take no unreasonable risks
- Avoid any sudden or unexpected movements or anything which a criminal may construe as a signal
- If you have been issued with a smoke pack, include it with any money that is handed over
- Use the 'SNAPSHOT' technique (see right) to help you to make a mental note of the appearance of the criminal(s)

Sex	Male/female
Nationality	Caucasian, Afro Caribbean, Asian, Indian, other
Age	Look for clues around the eyes and neck
Physique	Estimate the height, weight and overall build
Skin	Colour will help to distinguish race
Hair	Light, dark, straight, curly, thin, thick, sporting a moustache or beard
Outfit	Headgear, scarf, shirt, jersey, gloves, trousers, socks, shoes
Tattoos/scars	Tattoos are extremely useful as evidence. Note the type, the colour, location on the body

POL00423229

- Also make a mental note of any other possible evidence, such as likely fingerprints, shoe impressions, fibres or items of clothing.

After a hold-up

- Take time to calm yourself
- Lock the door
- Observe the getaway from a position of safety, if possible but do not put yourself at risk
- Telephone the police and give the following information:

- the name and address of your branch
- whether there are any injuries
- how long it is since the criminals left
- any vehicle make, colour, model, registration number
- the direction of the criminals' escape
- the number of assailants or robbers
- any weapons used
- a description of the criminals

- Inform the NBSC about the robbery as soon as possible
- Then keep the telephone line free until the Police arrive
- Ask customers to remain on the premises as they are essential witnesses (if they insist on leaving, take their names and addresses)
- Ensure that anything handled or left behind by the criminals remains untouched, so that it can be used as irrefutable evidence.

23.3 Burglary

If you arrive at your branch and there are signs of forced entry, suggesting a burglary has taken place:

- Do not enter the branch
- Phone the Police and await their arrival before entering
- Contact the NBSC to report the incident.

When you discover a burglary has taken place after you have entered the premises:

- Phone the Police on 999 as soon as possible
- Take care not to disturb anything that could be used in evidence
- Contact the NBSC to report the incident.

23.4 Emergency evacuation

If you need to evacuate your branch for any reason (eg, in the event of a fire):

- Ensure that all customers are helped safely to leave the premises
- Ensure that all bulk cash and stock is locked in the main safe and withdraw the key

Please note: The sub postmaster/Branch Manager and staff are responsible for ensuring that all cash and stock is secured, providing that time permits and it is safe to do so.

- Ensure that all 'working' cash and stock is locked in the counter drawers and the keys withdrawn
- Check that all windows and internal doors are secured

POL00423229

- Lock the counter access door and parcel hatch and withdraw the keys

Please remember: The sub postmaster/Branch Manager must keep the safe key, counter drawer keys, counter access door and parcel hatch keys with them when leaving the premises.

- Check that all customers have left the branch before the front door of the premises is closed
- Contact the NBSC to report the incident as soon as possible.

24 Bomb threats and suspect packages

Terrorist attacks, and attacks by extremist campaigners or malicious hoaxers are designed to intimidate, disrupt, cause economic damage and in some cases cause injury or loss of life.

There are many good reasons for planning for such situations, but there are also legal obligations for companies to do this under the Health and Safety at Work Act 1992.

These regulations state that:

- all employers are obliged to provide an environment where all reasonable care has been taken to safeguard the wellbeing of staff and visitors
- the responsibility for safety on premises rests with the employer and not the police
- appropriate procedures must be in place in the event of serious, imminent danger
- there should be persons competent to implement the procedures (ie one who has sufficient training and experience or knowledge to do what is required of them)
- employees must be informed of any possible hazards and the steps to be taken
- in the case of serious, imminent danger, work must be stopped immediately with people being moved to a place of safety
- access must be restricted, and resumption of normal work prevented, while the serious and imminent danger persists

24.1 Bomb Alerts

Bomb Attack

Where an explosive device explodes at or in very close proximity to a Post Office site or an explosive device is discovered at or in the very close proximity of a Post Office site.

Please note: A Post Office site is a Post Office, Post Office Cash Centre, Post Office Cash in Transit depot or any other building or area where Post Office Ltd business is conducted.

Bomb Hoax

A bomb hoax is where a bomb threat has been received, or a device or package is found and subsequent investigation by the Police or other agencies reveals that the device or package is a hoax.

Please note: Please treat all incidents as real until such time as the Police declare the incident a hoax.

Bomb Threats

A bomb threat is the suspicion or notification by a reliable source that a bomb has been planted inside or in close proximity to a Post Office Ltd site.

POL00423229

Crown Offices

Responsibilities

The Branch Manager:

Responsibility in the event of a bomb alert lies with the Branch Manager, or their nominated deputy until such times as the authorities deem it appropriate to take command.

- must formulate the Search and Evacuation Plans for their branch
- should have access to all relevant documents, such as the plans of the branch, at short notice
- should report all bomb alerts to the NBSC, initially by telephone
- will be responsible for checking that an up to date list of qualified first aiders at their branch is displayed
- must encourage the voluntary assistance of first aiders for a potential emergency situation
- must contact the Police whenever a suspicious item is found or when a bomb warning is received

The Police

The Police must always be contacted whenever a suspicious item is found or when a bomb warning is received. They will attend as quickly as possible and normally take command of a situation when they arrive on site. The Branch Manager should always offer them full co-operation.

The Police and armed forces are not responsible for searching for bombs which may be contained in the mail or placed within Post Office buildings. The task should be performed by search teams formed of local staff who have been appropriately trained in search techniques.

Once a suspect item has been identified, the Police will arrange for it to be examined and, if necessary, dispose of it.

Planning for bomb alerts

The Branch Manager must organise volunteers who will control evacuations, if this is considered appropriate and search the building in the event of an alert situation.

Plans specifying evacuation routes and assembly points outside the branch must be prepared. Special attention should be paid to the needs of handicapped or infirm members of staff when drawing up procedures. Work colleagues should be consulted to ensure assistance is readily available in the event that an evacuation is deemed necessary.

Please remember: Objects suspected of being bombs must not under any circumstances be touched or moved.

Building security, and staff security and awareness

It is always possible for a bomb to be introduced into or placed outside a building.

However, good housekeeping will enhance security, and items or structures which could conceal a bomb should be removed or kept to an absolute minimum (eg rubbish must not be allowed to accumulate). Public areas must be kept free from displays or objects which could conceal a bomb (eg display boards, Christmas decorations etc).

Special attention should be paid to security of access to vulnerable areas such as fuel storage rooms, boilers and central heating and ventilation installations. Whenever possible such rooms should be kept locked.

Evacuation routes must be kept clear of obstacles at all times. Clear plans for evacuation must be in place and fully understood by all staff.

Staff should be encouraged to report any suspicious circumstances to the Branch Manager. They should be encouraged to be vigilant for unusual objects (eg unattended packages which are apparently out of place).

Please note: The primary consideration in the management of a situation must be the safety of the staff and customers. Cost and service considerations are important, but ultimately must be secondary to safety of personnel.

POL00423229

Telephone threats

One activity adopted by activists, who seek to terrorise the population in order to gain their ends, is to phone organisations to make a threat of an imminent bomb attack.

Their calls generally fall into two categories:

- threats that actual devices have been planted; the aim of the terrorist in this instance is to be able to blame others for inaction if there are casualties
- threats where no device has been planted; the aim is solely to cause severe disruption

Even though most telephone bomb threats are made by malicious pranksters whose threats are empty, the making of these calls is a crime and must always be reported to the Police.

All bomb threats must be taken seriously and treated as genuine until they have been assessed.

The receipt of a threatening call can be a stressful experience for the recipient. It is difficult to remain calm when receiving a call of this nature but careful planning and training will help you to capture the content of telephone bomb threats, as this detail will allow a full assessment of the threat to be made.

Assessing the threat

The information captured during a telephone threat must be analysed immediately afterwards so that a judgement on the next course of action can be taken. Liaison with the Police is essential at this point as they may already be in possession of relevant information.

- Try and keep the caller talking and try to alert a colleague if possible
- Write down as carefully as possible the words used by the caller.
- Record the date and time of the call and the phone number on which the call was taken.

Try to find out the following as the call is being made:
The whereabouts of the bomb
What time it is due to go off
What the bomb looks like
What kind of bomb it is (eg explosive/incendiary)
What will cause it to ignite (timer/remote/chemical)
The identity of the caller
Why they are carrying out this threat
The sex, age and nationality of the caller
Whether the caller had a distinctive accent
Their likely state of mind (ie irrational? Incoherent? Rambling? Distressed? Drunk?)
Whether they were reading from a prepared statement or whether the message was taped
Whether there were any distinctive background noises (eg traffic, planes, machinery)
Whether it was an internal or external call, and whether a private line, mobile telephone or phone box was used
Whether a code word was given and what it was

The answers to these questions and any other information you can get will help in assessing whether the threat is genuine.

POL00423229

Responsibility for judging the credibility of a telephone bomb warning and the need for precautionary action rests with the Branch Manager in liaison with the Police. Bomb warnings should always be taken seriously and threat assessors should err on the side of caution until the threat has been fully assessed (ie threats should be treated as genuine until proved otherwise).

Experience shows that hoax calls greatly outnumber genuine calls. However, there are no easily defined common characteristics of a non-credible call although in most cases of hoax calls, the caller contacts the target direct. The genuine terrorist, however, will nearly always contact a third party (eg the press, a TV company, etc) and it is very unlikely that a terrorist warning would be received directly by the target site or organisation.

Warnings received by the Police or other authorities should always be treated very seriously.

Specific details contained within a warning increase the likelihood of the threat being genuine. Some calls, though, may come from people with a grudge against their local branch, the Post Office in general, or may even come from a disgruntled employee seeking to cause disruption to the service. Factors such as age and state of mind of the caller will influence the assessment and credibility of the threat.

As well as collecting any information you can at the time the bomb threat call is made, at this stage it may also help you to consider the points you have recorded on any comprehensive bomb threat checklist you have kept in your branch (see 'Action to be taken on receipt of a bomb threat' below) in order to determine whether the threat that has been made is likely to be genuine.

Action to be taken on receipt of a bomb threat (Bomb threat checklist)

It is advisable to keep a comprehensive checklist of all the information that you may want to consider if you receive a bomb threat in order to help you decide if the threat is genuine. You should keep this checklist near to your telephone so that you know it is easy to find, should you need it.

The points that you should record on your bomb threat checklist for consideration are as follows:

Bomb threat checklist:
The time and date of the warning
The method of communication (eg, by phone, by letter, via the Police)
If the threat was made by phone, with whom was the contact made (eg, to Headquarters, to the Police, the Press)
The exact wording of the threat
The current level of security status of your building with regard to likely threats
The Police's assessment of the credibility of the threat
Whether the threat is similar in nature to any other recent threats that have been made and whether other threats have proved genuine
Whether you are experiencing any industrial relations problems
Whether there are any special events taking place that are likely to encourage hoax calls (eg, political meetings, controversial social gatherings)
Whether the detonation time was specified
Whether the target details were specific and correct
Whether the location of the bomb was specified
Whether the type of bomb was specified (ie, explosive, incendiary)
Whether the container where the bomb is located was described
Whether any terrorist organisation admitted responsibility

POL00423229

Bomb threat checklist:
Whether any specific code word was given
Whether any specific demands were made (eg, political, financial)
Whether you are likely to be considered a high profile target
Whether your premises are particularly vulnerable to attack

The decision as to what action to take in the event of a bomb threat (whether by telephone or other means) lies with the Branch Manager in consultation with Senior Management via the NBSC. It is accepted practice for decisions to be taken by the most senior manager on duty at the time of the threat.

They will base their decision on the assessment of the call and will take advice from the Police.

There are three main options available to them:

- to take no action
- to undertake a search (see below)
- to evacuate the building (see 'Evacuation of the building' on page 91)

It is vital to ensure that other occupants of the building are kept informed of the situation.

The answers to these questions and any other information you can get will help in assessing whether the threat is genuine.

Always report bomb threat calls to your branch manager or the NBSC and the police immediately, even if you believe that it may be a hoax.

Searching for static bombs

Who should search

The main qualification for searchers is the willingness to undertake the task along with a familiarity of the place which they are searching.

The Police will not normally search premises following a bomb threat. They are not familiar with the premises and layout and would not be aware of what should be there and what is out of place. They could not therefore search as quickly and as thoroughly as people who work there all the time.

What to look for

Explosive and incendiary devices can be disguised in many different ways. Searchers do not have to be expert in devices. Their role is to look for anything unusual that should not be there, that cannot fully be accounted for, or that is out of place.

Search plans and how to apply them

It is vital that searches are conducted in a systematic and thorough manner. Searchers need to practise in order to familiarise themselves with their areas and to assess the length of time that a search is likely to take.

Search plans should be in place for all buildings and all search teams should be familiar with them. The objective of the search is to make sure that the building is checked as quickly and effectively as possible. If the building is not searched properly, there is no way of knowing if it is safe to reoccupy. Searching would be slow, costly and stressful for all concerned if no plans were in place.

The first step in preparing a plan is to divide the Crown Office into sectors. Each sector must be of manageable size for one or two searchers.

Areas where the greater number of public or staff are likely to be vulnerable should be searched first. Public areas to which a terrorist would have easy access should also have priority. Car parks, (if any) and outside areas and the perimeter should also be checked.

Depending on size, the sector may be one large room or perhaps a number of smaller rooms. Cloakrooms, stairs, corridors, car parks and other areas outside the building must also be included in the search plans.

POL00423229

What to do if something is found

The searcher who finds a suspicious item must not move it or interfere with it in any way. They will need a pre-planned way of communicating what has been found to the Branch Manager. Action thereafter will depend on the nature of the item and its location. Searchers must be reminded to observe the following rules:

- not to touch or move the item
- to move away from the item immediately
- to communicate what has been found to the Branch Manager

The Branch Manager will need to decide at this point whether to implement a part or complete evacuation of the building. The Branch Manager and the searcher who found the suspicious itemmust remain on hand to brief the Police on the location and description of the item.

Evacuation of the building

The evacuation itself may be a full evacuation of all staff to the outside of the building, or an evacuation of all staff except for the search teams.

The purpose is to move people from an area where they might be at risk of injury to a place of lesser risk. Occasionally it may be considered safer to stay inside a building rather then evacuate (eg if there is a suspicious item or vehicle outside the building).

The decision to evacuate requires careful consideration and will normally be taken by the Branch Manager. In exceptional cases the Police will insist on an evacuation and will require assistance from the Branch Manager to implement this.

Evacuations may take place in response to the following: situations:

- a threatening call made directly to the building
- a threatening call received elsewhere and communicated to you by the Police
- the discovery of a suspicious package (eg postal device or holdall, etc) in the building
- the discovery of a suspicious item or vehicle outside the building
- the discovery of an external device which is notified to you by the Police

Planning

Evacuation plans will allow the Branch Manager to react sensibly in a threatening situation. The plan will depend on the size and location of the building, the arrangement of the rooms, the number of exits and the amount of public access.

All plans must appoint and arrange:

- the designated evacuation routes and exits from the branch
- an assembly area at least 500 metres away from the building
- designated staff to act as marshals and/or contact points once the assembly area is reached
- general training on evacuation practices for all staff and specific training for staff with particular responsibilities

Re-occupancy

The re-occupancy of a building must always be discussed with the Police and when appropriate, other emergency services.

The safety of staff and customers remains paramount. Consideration must always be given to the likelihood of a secondary device, or the possibility that the vagueness of a threatening call may have led to confusion over the whereabouts of a device or the likely time of its detonation.

If an explosion or fire occurs, a building may be structurally unsound. In this case the damage to power and gas may render the environment unsafe, and advice should always be sought from Property Holdings. The building will also become a crime scene and access to it will then be limited.

POL00423229

What to do if a threat proves genuine

The Branch Manager must **immediately** contact the Police (if not already done so) and the NBSC if any of the following situations occur:

- a bomb explodes on Post Office premises, the Police believe that a suspect item on Post Office premises is a bomb or an explosive ordinance officer (bomb squad officer) decides to disarm a suspicious item
- a postal bomb explodes or ignites, or if the Police confirm that a letter or packet which has come in the post is an explosive or incendiary device
- your branch is evacuated as a result of a bomb alert

If the situation involves a postal packet, the following information should be obtained, whenever possible:

- the address on the item and a description of the writing
- its size and appearance
- anything about the packaging or 'make up' of the packet that may have looked suspicious
- the method of posting and the amount of postage
- the date, time and place of posting
- any injuries sustained

Publicity

No publicity should be given to any bomb threat, explosion, fire or false alarm.

The media will normally make persistent efforts to obtain witness statements and site photographs in the event of an explosion or fire. Staff should be warned not to answer any questions as the information may be misinterpreted in some way or may be sensitive in terms of the ensuing police inquiries.

All enquiries from the media should be directed to the Royal Mail Group Newsroom via the NBSC.

24.2 Suspect packages

All branches

Sometimes a terrorist or criminal seeking to cause personal injury and/or damage to property may conceal an incendiary device inside a package. The intention is generally that the device will explode as the package is opened but these devices may also a risk to life and limb while in transit.

The discovery of letter bombs in a Post Office branch is fortunately a very rare occurrence, as terrorists are unlikely to risk identification by posting them in person. For this reason, they are more likely to post them in letter boxes.

However, for safety reasons, it is advisable to be able to identify a package that may contain a letter bomb.

Recognising a suspect package

The following points may help you to decide whether a package may contain suspicious contents:

Dimensions of the package	A letter is unlikely to be less than 3mm (1/8") thick, or weigh less than 43 grams (1½ ounces)
Balance of the package	Lopsided packets should be treated with suspicion; packets that are disproportionately heavy for their size could contain an improvised explosive device
Holes or stains in the packaging material	Packets with grease stains or pin holes in the wrapping should be treated as suspect
Smell	Some explosive materials smell of marzipan or almonds
Noise	Ticking or hissing sounds may indicate the presence of an improvised explosive device

POL00423229

A flap on the package	Check whether the wrapping completely stuck down; normally there is a small gap at the end of the flap
The type of envelope used	Experience has shown that letter bombs are usually found in 'Jiffy bag' type envelopes
Excessive packaging or postage	Check whether an excessive amount of wrapping or sealing has been used or whether more postage than necessary has been affixed
Appearance of contents	If, in addition to any other suspicious factors, the appearance of the package suggests that it could contain a book or video cassette, it should be treated as suspect

What to do if you discover a suspect package

If you examine a package and believe that it may contain an explosive device:

- Leave the package undisturbed on a flat horizontal surface
- Warn everyone in the immediate vicinity and close the branch
- Contact the Police and seek assistance
- Notify the NBSC that the branch has been closed.

Do Not

- Drop the package or throw it away
- Attempt to open the package
- Bend or flex the package in an attempt to discover the contents
- Immerse the package in sand or water
- Place it under a sandbag or other heavy object
- Place the package in any container other than one specifically designed for this purpose (ie, a bomb tube to which branches attached to a sorting office may sometimes have access)
- Handle the package more that is absolutely necessary.

Members of the public returning a suspicious package

If you are asked by a member of the public to take back a package which they have had delivered because they are suspicious of the contents:

- Do not accept the package under any circumstances
- Advise them to contact the Police.

24.3 Chemical, Biological, Radiological, Nuclear (CBRN) and White powder incidents

Please use the following procedures when dealing with a Chemical, Biological, Radiological, Nuclear (CBRN) or White powder incident:

- If a letter, parcel or package is found to be leaking powder or liquid by a member of staff you must make a risk assessment (without putting yourself at risk) based on visible contents, markings, leaks or residue, postmark and addressee using the suspect package check-sheet, see para 24.2.
- If the item is suspicious, please use the following processes:

Powder (any colour), sand or fine granules leaking from the item

- Call the Police on 999 stating 'White powder incident'.

- Move people away from package (at least 20 metres if in an open area) or out of the room.
- Shut down any air conditioning.
- Close all doors and windows.
- Isolate the area.
- Identify people who have been within 20 metres of the item.
- Classify affected people as:

- Primary - Direct Exposure
- Secondary - in same building
- Tertiary - passed through building.

Once the emergency services have been called:

- notify the NBSC on GRO selecting option 1.

Liquid or liquid residue leaking from the item

If there are any immediate symptoms such as dizziness, shortness of breath, nausea or burning sensation around the eyes and mouth:

- Call the Medical Services on 999 stating 'Chemical incident'.
- Call the Police on 999 stating 'Chemical incident'.
- Evacuate the area.
- Follow the process for 'Powder (any colour), sand or fine granules leaking from the item' (shown above) from the bullet that says 'Shut down any air conditioning'.

Please note: If you are in a multi-occupancy building you must notify other tenants/occupants of the incident.

Members of the public

You cannot insist that a member of the public who has been involved in a 'CBRN' incident remains in your branch. If they wish to leave the area, they must be allowed to do so. However you must ask them to provide their name, address and telephone number so that the emergency services can contact them should they wish to do so.

25 Hostage policy

All branches

Post Office Ltd has a long established hostage policy for all staff, sub postmasters and agents. The primary objectives of the policy are the safety of any hostages that may have been taken, and the safety of anyone else who may be involved.

It is not possible to anticipate precisely the method in which a hostage situation may manifest itself. It could be by telephone, text message, written communication or by some other means. The message could be sent direct to an employee, to their family, or through a third party in one of the following ways:

- a person may be approached on their way to work and told that their family or someone close to them has been taken hostage; demands are then made and sometimes a photograph of the hostage is shown to the staff member to convince them that the threat is genuine
- a staff member may be told that their family has been taken hostage or kidnapped, and that money has been demanded for their release
- a staff member may be kidnapped away from the workplace, and money demanded from other staff or colleagues
- an employee and their family may be seized at home, and the employee is then directed to return to work (usually the next morning) to obtain cash and deliver it to the criminals at a pre-determined location
- an employee and their family may be seized at home and the employee is then escorted to their office or place of work under threat; access to the work place is gained under duress and cash is then targeted directly by the criminals

POL00423229

These situations are frequently referred to by the Police and the retail/cash industry as 'Tiger kidnaps'.

Please note: The hostage policy does not cover situations where a member of staff, sub postmaster, agent or customer is held at a Post Office branch with an immediate demand for money. In this instance the hostage policy does not apply as the situation is 'robbery with menace' and those involved are required to do whatever is safest in the circumstances for all concerned. At the first opportunity (ie, whenever it is safe to do so), the incident must be reported to the Police on 999 and to the NBSC.

Hostage Helpline Emergency Telephone Number

Experience has shown that the safest course of action in hostage situations is to call a dedicated helpline number and allow the incident to dealt with by trained staff.

For this reason, an emergency helpline number has been set up where you can get immediate support. The number is staffed 24 hours a day throughout the year.

The Hostage Policy telephone number is FREEPHONE 0800 1699988

Once a call has been received, you will be asked to provide brief details of the incident. You should try to remain calm and give whatever information you have available, as the primary objective is the safety of everyone involved. The hostage policy will then be immediately invoked.

If, for any reason, you are unable to call the hostage helpline, you should try to alert your manager to the situation. If this is not a feasible option either, you should call 999. If you do call 999, you must make it clear to the operator that you are reporting a 'hostage situation'. The use of this wording will ensure a discreet response.

The Hostage Helpline number must only be used for reporting hostage situations. It must not be used to report other incidents such as burglaries, robberies, alarm malfunctions, etc.

Misuse of the number could block the line when a genuine caller is attempting to get through. All calls are taped and may be used in any subsequent Police enquiry.

The number must not be given out to members of the public, nor should it be displayed where customers can read it.

If you find yourself in a hostage situation:

Do

Telephone the emergency number if it is safe to do so
Try to remain as calm as you can
Try to establish a relationship with the people who have taken you hostage (this may help to reduce tension)
Stay alert and concentrate on what is happening
Try to remember the physical features and clothing of your captors

Don't

Resist physically as you or your family could get hurt
Show hostility or provoke your captors
Refuse to talk

POL00423229

26 Screen-less working and its benefits

Following attacks using corrosive liquids that were prevalent for a relatively brief period during the 1960s, a perception grew that only a full separation of the counter staff from the public could ensure the safety of staff and the security of assets, and as this perception became common currency in the 1970s and 80s, counter screens were increasingly employed in Post Office branches as the normal working environment.

However, since the 1990s when the Post Office began a trial of early 'open-plan' environments (as screen-less layouts were then known) in a number of Crown or Branch Offices and at the same time encouraged some forward-looking sub postmasters to install a similar design, the move towards the adoption of a screen-less working environment has continued to gain greater currency within Post Office Ltd, and indeed with its competitors, such as banks and building societies. Equipment manufacturers have made significant advances in the design and development of cash management machines and Post Office Ltd now uses a wide range of smaller, lighter and more efficient units, many of which are designed to work as night safes as well as a convenient means of daytime cash storage and protection.

While the introduction of the various screen-less formats has always been undertaken with a careful regard for the security of staff, customers and Post Office assets, experience has proved consistently that screen-less branches suffer lower levels of attack, lower levels of loss when attacks do occur and no attacks that have resulted in any significant injury to staff or customers.

Benefits of screen-less working

The following security-related benefits of working in a screen-less environment have been identified as the following:

Lowered risk of a robbery

In recent years the number of screen-less branches has reached a level suitable for statistical analysis.

There are currently over 1000 branches containing no counter screen, or one or two screened positions only for high value cash transactions, and the latest feedback shows that levels of robbery in screen-less branches are less than half those that are reported in branches with screens. In addition, levels of loss on those occasions when an attack is successful (for the robber) are significantly less than for successful attacks against screened branches.

Please remember: A reduced level of loss generally results in less likelihood of repeat victimisations and consequently a reduced potential of trauma for counter staff and customers.

Increased security for assets

In screen-less branches less cash is readily available than in a screened environment where all cash required for the day's trading is more easily accessible.

The whole process of cash management is more secure as most of the cash requirement for the day (apart from an amount of up to £600 which is available in the Flip Top Till) is stored in Cash Funding Units (CFUs) which dispense pre-determined amounts of cash with a time delay between each withdrawal.

These features contribute towards a more secure working environment by making it potentially less attractive for thieves and robbers to perpetrate a crime.

Improved working and sales environment

While it has never been possible to measure accurately the levels of aggressive behaviour, not related to theft, exhibited by customers in branches with counter screens, the frequency with which this issue is raised by staff in screen-less branches suggests that improvements in the staff/customer relationship in an open plan environment are significant. This is undoubtedly enhanced by the more intimate surroundings brought that encourage customers to feel more relaxed about their shopping experience.

POL00423229

27 Format of the counter

There are a number of options for the type of counter that is used for a screen-less working environment. Linked to these options are some specific security requirements that depend upon the amount of business your branch carries out.

The most popular options are described below.

Screen-less counter

This counter has no screen and provides a pleasant working environment for staff and customers. A Cash Funding Unit and a Flip Top Till are essential items of equipment to support this format of counter.

Transactions up to a limit of £600 can be carried out. A secure screened position or area may be required to house the main safe, for the acceptance of Remittances and to carry out individual transactions in excess of £600, if these are accepted. (see 'Mixed formats' on page 100). In addition, a back cupboard and parcel acceptance unit may also be required.

Dimensions of the screen-less counter

In order for you to decide whether this type of counter set-up is appropriate for your needs, the dimensions of its constituent parts are given below:

Item of equipment	Height	Width	Depth
Single position service desk (unseated)	975mm	1100mm	1130mm
Single position service desk (seated)		1648mm	1163mm
Double position service desk (seated)		2800mm	
Parcel pedestal	820mm	600mm	648mm
Counter pedestal unit	945mm	459mm	508mm
Cupboard (back of counter)	2100mm	1000mm	350mm

POL00423229

Combi counter

The Combi counter is designed to link into a retail counter to enable you to serve both Post Office Ltd and retail customers from the same area.

In the same way as the normal screen-less counter, a Cash Funding Unit and a Flip Top Till are essential items of equipment to support this format of counter. Transactions up to a limit of £600 can be carried out. A secure screened position or area may be required to house the main safe, for the acceptance of Remittances and to carry out individual transactions in excess of £600, if these are accepted. (see 'Mixed formats' on page 100).

In addition, a back cupboard and parcel acceptance unit may also be required.

Dimensions of the Combi counter

In order for you to decide whether this type of counter set-up is appropriate for your needs, the dimensions of its constituent parts are given below:

Item of equipment	Height	Width	Depth
Single position Combi (unseated) with retail service desk and basket well	975mm	2320mm	1130mm
Single position (seated) with retail service desk and basket well		2868mm	1163mm
Double position (seated) with retail service desk and basket well		4020mm	
Parcel pedestal	820mm	600mm	648mm
Counter cupboard	2100mm	1000mm	350mm

POL00423229

Screen-less sub office counter (SSOC)

This is a 'stand-alone' single unit designed for branches that carry out only minimal Post Office Ltd business or that are open for reduced hours of business.It is designed to be positioned alongside an existing retail counter.
A BiDiSafe and Drop Safe are essential items of equipment to support this format of counter. A maximum allowance of £6,000 in cash is operative each working day and you can carry out individual transactions up to £600 maximum.

The SSOC does not have sufficient room for scales, so you will need to ensure there is available space on an adjoining counter for these. Additionally, you will need to provide a shelf under an adjoining counter for locating the main Horizon A4 printer if your branch is a single position counter.

Ideally, the SSOC should not be located against a wall, since the wall would hinder the access to the drawers and countertop. If there is no other option, the unit can be placed against a wall to the left hand side of the unit (from the user's perspective). The unit should not be placed directly against a wall to the right side (from the user's perspective). If this is the only option, a 300 mm minimum space between the wall and the SSOC unit should be used; this space can be filled with a worktop if required.

An explanation of the design of the format is given below:

Top Drawer
Slam-shut lockable drawer. For the secure storage of your datestamp and stamp folio on retention units.

Second and Third Drawers
Slam-shut lockable drawers. For the secure storage of 'working stock' (eg, stamps, Phonecards, transaction documents, etc. The drawers should be as deep as possible to maximise the storage area.

Filing Drawers
MDF drawers, not lockable. To include a removable divider.

Security Drawer
Lockable drawer, with a separate key to the other lockable drawers. If necessary, for the overnight storage of the stamp folio, and temporary storage of coin and value stock when first delivered.

Flip Top Till (FTT)
The till will store cash up to the value of £600. It should measure 100mm (in height) by 327mm in width by 245mm in depth.

FTT controls and siting of Panic Alarm
The FTT controls are just above the 'two finger' operated panic alarm.

Cash Funding Unit (BiDiSafe)
Provides secure storage for banknotes.

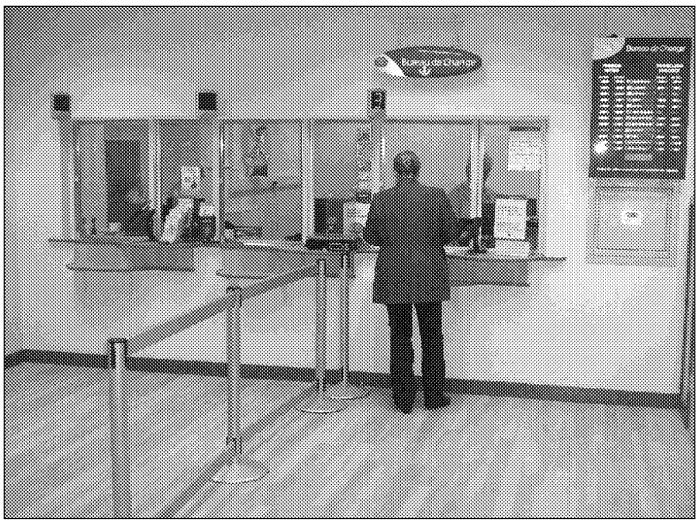
Safe
There are two options for the safe (both the same size). The type of safe selected depends on the amount of cash that needs storing.

CPU storage
The shelf permits space to store the Horizon CPU and allows adequate air circulation space. The shelf should have no backing and be at least 550 mm deep.

Overall dimensions: height 1000mm, width 780mm, and depth 850mm (including the front lip 100mm).

POL00423229

Mixed formats



Different formats can be combined to achieve the most suitable layout for your branch. This takes into account the fact that many screen-less branches will need to have a secure position fitted, to accommodate the main safe and for the acceptance of high value transactions (ie, over £600) and Remittances. The only exceptions to this are branches that have opted for the screen-less sub office counter with a drop drawer safe fitted.

With regard to the secure (fortress) position, it is recommended that there is a distance of 1850mm, or an unimpeded distance of 1500mm, from the back wall to the back edge of the counter. The counter depth is usually 1000mm, and to allow for the privacy of customers whilst being served, a space at least 1.500mm deep should be provided in front of the position from the head of the queuing area. An illustration of a secure (fortress) position is shown to the right.

As an example, in a branch with four counter positions you could have one of the following set-ups:

Two fortress counters and two screen-less or Combi counter positions. This will enable you to accept large business deposits and Remittances in the fortress area and manage normal Post Office Ltd business at the screen-less or combi counters. The Combi counters enable you to economise on staffing, as staff at these counters could serve both retail and Post Office Ltd customers and you will have the option of extending your Post Office Ltd hours to pick up extra business after the normal Post Office Ltd area closes. By using two non screened or combi counters you will only require one Cash Funding Unit.
One fortress, two screen-less and one combi counter position. This means that you can accept Remittances and large cash deposits at the fortress position, and also have the flexibility of two screen-less counter positions for normal Post Office Ltd business, and a combi counter which could help with serving customers at times of pressure, and could stay open later than the main counter area to attract out of hours business. This option requires two Cash Funding Units, one to serve the two screen-less positions and another for the combi counter position.

Please remember: If your Post Office Ltd work is minimal, you could consider a SSOC unit instead of the combi counter.

28 Security equipment that is required

The following equipment should be installed in a screen-less working branch:

All screen-less branches

Cash Funding Unit

The Cash Funding Unit has a time control for the management of cash deposits and withdrawals. The type of Cash Funding Unit that is installed must be determined by the amounts of cash that you pay out, not the levels of cash declared in your overnight cash holdings.

Some examples are illustrated below:

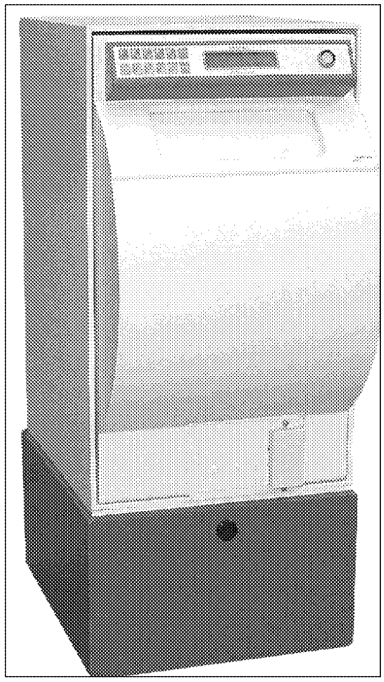
POL00423229

RollerCash unit

The RollerCash unit has a rotating central drum with **20** segments, each capable of holding £1200 (2 X £600). Segments are accessed one at a time through an opening protected by a motorised shutter. Users operate the RollerCash with a multi-functional keypad on the front of the unit just above the shutter. The unit can be set so that more than one user can operate it at the same time.

An LCD (Liquid Crystal Display) assists in the operation of the Rollercash by providing the appropriate prompts, warnings and messages.

Please note: The new design RollerCash units do not include the top drawer and the Drop Safe is optional.

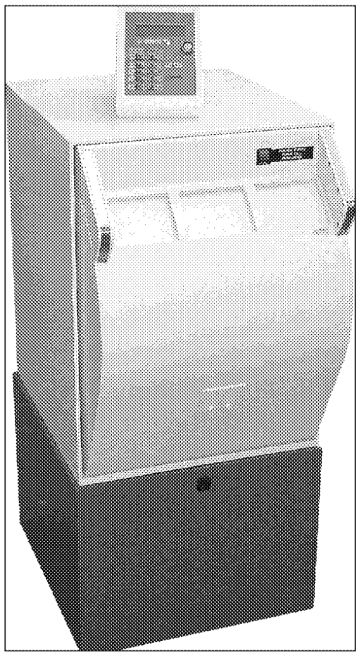


RollerCash

RollerCash with Drop Safe

RollerCash Trio

The Trio is the same as the other RollerCash unit except that it has a rotating central drum with **30** segments, each capable of holding £1200 (2 X £600), and the multi-functional keypad is sited on the counter desktop.



POL00423229

Robocash

The Robocash unit has a series of 40 revolving cassettes, each capable of holding £1200 (2 X £600). Segments are accessed one at a time through an opening protected by a motorised shutter. Users operate the Robocash with a PIN code on the multi-functional keypad on the front of the unit just below the shutter. The unit can be set so that more than one user can operate it at the same time.

An LCD (Liquid Crystal Display) assists in the operation of the Rollercash by providing the appropriate prompts, warnings and messages.

Flip Top Till

The Flip Top Till (see illustration on the right) is limited to the secure storage of a maximum of £600 at any one time. An alarm sounds if the Flip Top Till is left open for longer than 20 seconds, and this can be linked to the office alarm. The till locks down when this is activated.

It should measure 327mm (in width) by 245mm (in depth) by 100mm (in height).

Retention Units

The Retention Unit is basically a chain that secures the datestamp and the stamp folio to the counter, to prevent them from being grabbed and removed by members of the public.

Hampers/End Gates

Hampers are perspex, acrylic or polycarbonate barriers fitted on all screen-less counters, which are designed to protect the working space of the staff from intrusion and to prevent the snatching of items on the counter (please see illustration below).

End Gates are used to prevent unauthorised access behind the counter.

POL00423229

Alarm

A EA2K monitored alarm system should be installed in branches with an overnight cash holding that exceeds £6, 000. All bandit alarms are silent in a screen-less branch, even in the secure accommodation.

Drop Safes

These are optional but should be installed in branches that carry out transactions in which cash is frequently accepted and requires depositing immediately.

Screen-less sub office counter (SSOC)

Safe

There are two options for the safe (both the same size) in an SSOC. The type of safe selected will depend on the amount of cash stored at the branch.

If the weekly total of cash from deposits, overnight cash holdings, and Remittances in your branch is £6,000 or more, a Drop Safe is fitted, and cash and stock must not be stored overnight. Cash and stock items must be removed from the unit and placed into the main safe instead. With this set-up an EA2K Alarm system is installed, with silent personal attack buttons linked to the system sited at the counter positions at the screen-less counter.

If the weekly total of cash from deposits, overnight cash holdings, and Remittances in your branch is less than £6,000, a Drop Safe Drawer should be used, and cash and stock can be stored overnight. In this instance the branch will have a silent personal attack button provided on the screen-less working desk.

Cash Funding Unit (BiDiSafe)

The BiDi Safe provides secure storage for banknotes (see illustration on page 99).

Security drawer

This must be lockable. There must be a key to other lockable drawers, if necessary, for overnight storage of stamp portfolio and coin and value stock when first delivered.

It should measure 780mm (in width) by 1000mm(in height) by 245mm (in depth), including the front lip of 100mm.

POL00423229

29 General security procedures

Please note: When the Cash Funding Unit is mentioned, this applies to whichever type your branch has been supplied with (ie, BidiSafe, RollerCash, RollerCash Trio or Robo 40).

Cash float

There should never be more than £600 at risk at any time at the counter position.

For this reason, the Flip Top Till must be limited to hold £600 cash at any one time.

Any other available cash exceeding £600, including any deposits that are accepted, must be dispensed in the Cash Funding Unit or the Drop Safe. The maximum that can be contained in a BiDiSafe is £300 per cassette or £600 per slot in the Rollercash, Trio or Robo 40.

Cash Funding Units

BiDiSafe

- Always ensure that the arrangements for the loading and unloading of cash are implemented outside of business hours with the front door of the branch locked.
- Always secure the main door keys to the BiDiSafe in the Main Safe except when you are loading and unloading it

The amount of cash that is held in the BiDiSafe during the day must never exceed £6,000 (20 cassettes X £300).

The maximum amount of cash that the BiDiSafe can dispense for each request must be limited to £300; therefore, a request for further funds from the BiDiSafe must only take place once it is below £300.

After a request for cash, a £300 cassette will be dispensed with a time delay of 10 seconds. The time delay for the release of any subsequent amount requested immediately is 60seconds.

Please remember: This Cash Funding Unit must not be used for overnight retention of cash.

Rollercash, Rollercash Trio and Robo 40

Two or more users can operate one Cash Funding Unit at the same time.

The loading and unloading of cash for these units must be implemented outside of Post Office® and retail business hours with the front door of the branch locked.

Each of these Cash Funding Units can be used for overnight retention when the case complies to European grade 0 safe protection and Post Office approved standards (in the case of Rollercash units, up to a maximum of £24,000 and in the case of Trio and Robo40 units, up to £30,000). When these standards are not in force, cash must be secured in the main safe in the back office and the alarm system set before you leave the branch.

The maximum amount of cash that can be held during the day is:

- in the case of the Rollercash, £24k (20 slots x £1200)
- in the case of the Rollercash Trio, £36k (30 slots x £1200)
- in the case of the IBP/APL Robo 40, £48k (40 slots x £1200)

The maximum amount of notes that the unit can dispense for each transaction is £600 (when a £1200 slot is accessed, £600 should be re deposited in the same slot). As the maximum amount available in the Flip Top Till must not exceed £600, a request for further funds from the Cash Funding Unit should only take place once the top drawer contains less than £100.

Please note: The programming of the Cash Funding Unit will reject requests for figures relating to deposits or withdrawals that is higher than £1200.

Withdrawal Slots A,B,C and D can be dispensed with a time delay of 5 seconds. The time delay for the release of any subsequent amount of £600 requested immediately is 30 seconds and in the case of withdrawal slot E, the time delay is 120 seconds.

The total withdrawal wait time is 15 minutes (900 seconds). This can only be put into operation after the close of business.

POL00423229

'Multi-user' total withdrawal can be carried out after the normal total withdrawal time of 15 minutes using the manager's key. When not in use, the keys to the Cash Funding Unit must be secured in the main safe.

Training for these units

For more detailed information, please refer to the Rollercash or Rollercash Trio quick reference guides.

Drop Safe

The Drop Safe consists of a top (drop) slot capable of accepting small bundles of notes and small bags of coin. All cash in excess of the £600 float must be deposited in a Drop Safe or re-deposited into the Cash Funding Unit.

Cash must be removed from the Drop Safe and stored in the main safe outside of business hours.

The main door of the Drop Safe is fitted with a key lock.

Counter transactions

Transactions must be completed as quickly as possible. Cash, secure stock, documents, etc. must always be secured in the Flip Top Till, the Cash Funding Unit, the Drop Safe, or drawers, as appropriate as soon as possible, to avoid theft.

Please remember: Cash, stamp folios and documents relating to transactions must never be left on top of the free-standing desk.

Confidential documents must not be left where customers can read them. Mail must be kept in a secure place out of reach of the general public.

Stock holding

All holdings of stock, licences and other value items must be kept to the minimum level, which will meet the requirements of providing an efficient service to the customer. Obtaining additional holdings during the day is preferable to overstocking.

At the close of business all cash, and value and secure stock items must be withdrawn from the Flip Top Till, the BiDiSafe and desk drawers and secured in the main safe.

Motor Vehicle Licences (MVLs)

Motor Vehicle Licence discs must be kept to an operational minimum at the open plan counter and must always be kept in the lockable top drawer of the desk.

At the close of business:

- Remove all Motor Vehicle Licence discs from the open plan position and secure them in the main safe.

Business deposits

Business deposits up to a maximum of £600 should be accepted at the counter and deposited into the Drop Safe immediately.In the case of transactions over £600 (both deposits and withdrawals), these must be accepted at a dedicated secure position.

Key security

Keys to the desk drawers must not be left in the locks at any time. The desk drawers (fitted with 'slam shut' locks) must be closed whenever you need to leave the desk, regardless of the length of absence. The BiDiSafe main door key must be kept in the main safe except when you are loading or unloading the unit outside of normal business hours.

Datestamps/stamp folios

Datestamps and stamp folios must be secured using the Retention Unit on an 'under' counter shelf when not being used. If a desk is left unattended for any length of time, the datestamp/stamp folio must be secured within a locked drawer.

POL00423229

30 Security instructions

Core and Outreach services

The definition of a Core and Outreach operation is the instance when a sub postmaster operates one or more sessions of service in various sites in addition to their sub Post Office (known as the 'Core' branch). There are four types of Network Outreach service: Mobile, Hosted, Partner and HomeService. A description of each type of service is given below.

In all cases the Outreach service is supplied by a local sub postmaster whose 'Core' branch provides the central point of support by ordering cash, stock and leaflets, and answering queries. The sub postmaster is therefore known as the Core sub postmaster.

The Core sub postmaster will usually offer an Outreach service in more than one local community and in this case the group of services is known as a cluster. The opening hours and the products and services on offer vary according to the type of Outreach service that is being operated.

This section of the booklet explains any security procedures relating to Network Outreach sites that are not covered in relation to requirements for 'Core' branches.

For full details of how Outreach sites operate on a daily basis, see the Network Outreach services booklet. Security instructions for 'Core' branches can be found in the relevant sections of the rest of this booklet.

Please note: It is not intended that the instructions in this document should replace any existing business rules for specific products and services that are published in the individual booklets of the Operations Manual. For this reason, reference is made to these booklets throughout the contents of this one.

Branch types

Mobile vans

This is a travelling Post Office® sited in a mobile van that delivers core products and services to customers in small communities at set times and days each week.

Hosted service

A fixed site Post Office branch in which the sub postmaster or his assistants will offer core Post Office products and services during restricted hours each week. The premises are owned by a third party, such as a shop or a community centre.

Partner service

A fixed Post Office® location in local business premises such as a pub or retail outlet in which the owner offers a range of Post Office products and services to customers.

HomeService

Post Office® HomeService is only available in clearly identified communities and there is no physical branch at the Outreach location. Instead, the sub postmaster fulfils customers' orders in one of the following ways:

- by delivering the order to the customer's home
- by sending the relevant items relating to the product or service through the post
- by holding a local 'drop-in' session

The sub postmaster does not fulfil orders to customers outside of these identified communities.

For information on Mobile vans, Hosted and Partner services, see the Network Outreach services booklet. For information on HomeService, see the Post Office® HomeService booklet.

POL00423229

Equipment

Cash Carrying Case

Two Cash Carrying Cases with a dye degradation system are in operation (one with a maximum cash holding of £6,000 and the other with a maximum cash holding of £15,000) and each Network Outreach Service provider will use the one that is appropriate for the value of cash that is being transported and the level of security risk attached.

The Cash Carrying Case must be used to transfer cash, Motor Vehicle Licences and Gift Vouchers (when available) from the 'Core' branch to the Hosted Outreach site(s). Whenever possible the Cash Carrying Case with the lower maximum holding of cash should also be used to transport value and secure stock, and any datestamps that are used from site to site. If this is not possible, an inconspicuous bag may be used to transport stock and datestamps.

Please note: Coin must never be transported in the Cash Carrying Case. It must always be carried in an inconspicuous bag.

The case is also used to provide secure accommodation for items except for coin on site, and must be kept out of site of the public.

Keys must not be transported with the case except in specific approved circumstances.

Full operating instructions for the case are delivered with the equipment, and training will be carried out before the case is used in each instance.

Mobile personal alarm (Skyguard)

Post Office Ltd supplies a silent personal attack alarm (see 'Portable panic alarm (Skyguard Mobile Lone Worker Protection System)' on page 51) to sub postmasters who carry items greater in value than £6,000. The alarm includes a monitored tracking device. The sub postmaster or member of staff providing the sessions of Post Office service must keep the mobile personal alarm with them every time they are operating one of the Network Outreach services, and in transit between locations.

All Network Outreach services

Transportation of cash and stock using the Cash Carrying Case

A low value or a high value Cash Carrying Case (see para 17.8 on page 60) is used to transport cash and stock from the 'Core' branch to the Outreach site, and vice versa, and to provide secure accommodation for cash and stock while in transit. The daily cash requirement (up to £6,000 or up to £15,000) will determine the type of case that is used.

Please remember: You should not carry cash in excess of £6,000 or £15,000, depending on the type of Cash Carrying Case in use.
If you ever need to transport cash to a greater value than the cash is designed to take (either from or to the 'Core' branch), you must telephone the NBSC to advise them that you are carrying more cash than the limit imposed for the Cash Carrying Case.

Depositing cash and stock in the case

Before you are due to transport the cash and/or stock (usually the night before you are travelling to your Outreach site(s):

- Divide the cash into separate bundles of £600 in mixed denominations
- Enclose the bundles in elastic bands (do not place them in plastic cash bags)

Please note: This is an essential requirement when you are using the Cash Carrying Case.

- Place all the cash, and secure stock for transportation to the Outreach site(s) in the safe overnight, but not in the inner '40 minute compartment' unless there is enough time to open this in the morning (you must not keep cash and stock in the Cash Carrying Case under normal circumstances)
- Ensure that the personal alarm (if supplied) and the cash case are fully charged for use in the morning.

Please note: If a personal alarm is not provided, the sub postmaster or the member of staff operating the service must carry a fully charged and working mobile telephone with them.

POL00423229

Securing the Cash Carrying Case and preparing for your journey

Just before you are due to leave the 'Core' branch:

- Remove from the main safe the cash required to operate the Mobile service for the day, the stamp folio (if not secured at the Outreach site) and any other stock that you need
- Place the following items into the secure compartment of the Cash Carrying Case:

- the cash
- the datestamp
- Vehicle Licences (if appropriate) and Gift Vouchers

Please remember: If there is not enough room in the High Value Cash Carrying Case for the datestamp, this can be placed in the inconspicuous carrying bag (see below).

- Secure and activate the case (see para 17.8, page 60), ready for transportation to the Outreach site

Please note: Keys for the Cash Carrying Case must not be carried with the case during transportation.

- Place your portable Horizon equipment, if applicable, in the boot of your vehicle first
- Then place any equipment you are using (other than the Cash Carrying Case) any forms and leaflets, and coin and stock in an inconspicuous carrying bag and place this in the boot of your vehicle

Please note: If there is any spare room in the low value Cash Carrying Case, it is preferable to place stock in the case rather than the inconspicuous carrying bag.

- Place the Cash Carrying Case in your vehicle, following the instructions in the User Manual, ideally in the passenger footwell or behind the front seats
- Get in the vehicle and lock the doors.

Please note: You must follow the instructions in this order when leaving the 'Core' branch in order to comply with security requirements.

While travelling to the Outreach location (in transit)

- Ensure that all of the doors of the vehicle used are kept locked
- Whenever possible, leave the 'Core' branch at a different time and use a different/alternative route to the Outreach site
- If a personal alarm has been provided, ensure that you keep this with you at all times.

Every effort must be made to minimise the risk of attack when you are in transit with items of value. This means that you should carry out refuelling of your vehicle before you begin your journey. You should avoid making a stop en route unless you need to refuel. Other than refuelling, the vehicle should be manned at all times. You must exercise extra vigilance when refuelling; if possible, refuelling should be carried out at a Royal Mail depot.

All circumstances that seem to threaten an accident or that cause the vehicle to slow down must be regarded with suspicion. Similarly, you should never allow the mobile van to be boxed in and should assess each situation as it occurs in case evasive action is required.

A process must be put in place at the 'Core' branch to ensure that the Cash Carrying Case and other items of value can be collected in the event of a vehicle breakdown or accident. For this reason you must also ensure that the mobile personal attack alarm, if provided, is carried by the operator at all times.

Please note: In the case of a mobile van, if you break down, you must contact the ARC and give the location of the vehicle and the nature of the breakdown. If you are advised to leave the vehicle, you should ensure that the surrounding area is safe before you do so.
The vehicle must not be left unattended or exposed to any potential criminal activity unless you are advised to evacuate the vehicle on a motorway and position yourself at a distance to await assistance. If possible, provision of an alternative vehicle should be made available.
If you have an accident in the van and you have no apparent injuries, you must remain in the vehicle and contact the ARC, stating your location. If you are present at the scene of an accident but not involved,

POL00423229

you must remain within the mobile van. You must not alight from the vehicle or open the doors. If the mobile van is seriously damaged in an accident and injuries are sustained, you should attempt to leave the vehicle and raise the alarm.

Upon arrival at the Outreach site

Please note: The instructions below will vary for the Network Outreach service provided on a mobile van. Please refer to the Network Outreach services booklet for full instructions for a period of service at a designated site in a mobile van.

- Park your vehicle as near as possible to the entrance of the Outreach site, to reduce the distance that you need to carry cash and stock
- Check as far as possible around the premises to ensure that no forced entry has been attempted and that there are no other suspicious circumstances
- Remove the Cash Carrying Case from your vehicle (re-locking the vehicle behind you) and take it into the service area in the Outreach site
- Locking the service area behind you (if possible), collect the mobile Horizon equipment and any other items from the boot of the vehicle
- Set up the Horizon equipment, if applicable
- Open the Cash Carrying Case and remove one bundle of cash (£600)
- Place the bundle in the lockable drawer

Please remember: Cash and value stock must always be kept in the lockable drawer provided.

- Ensure that the remainder of the cash and the bulk stock is kept in the Cash Carrying case and stored out of the view of your customers
- When necessary, replenish the 'working' cash from the Cash Carrying Case (this must be done discreetly, out of view of the customers or when there are none waiting).

At the close of business at the Outreach site

Please note: The instructions below will vary for the Network Outreach service provided on a mobile van. Please refer to the Network Outreach services booklet for full instructions for a period of service at a designated site in a mobile van.
In the case of Partner branches, if the cash to be stored overnight exceeds the acceptable level, the Partner branch must notify the Core sub postmaster who will make arrangements to transport cash back to the 'Core' branch (see 'Collecting surplus cash and stock (Partner branches only)'below).

- Secure the remaining cash that you need to return to the 'Core' branch, the datestamp, Vehicle Licence discs and Gift Vouchers in the Cash Carrying Case (ideally customer documents from transactions you have carried out and the datestamp should be secured in the Cash Carrying Case; if there is not enough space, you should use the inconspicuous carrying bag)

Please note: If you need to return cash to the 'core' branch to a greater value than the cash is designed to take, you must telephone the NBSC to advise them that you are carrying more cash than the limit imposed for the Cash Carrying Case.
In the case of Hosted branches, you can leave £600 in stock or coin (but not Vehicle Licence discs) in the lockable drawer.

- Place any remaining stock or coin in the inconspicuous carrying bag, ready for transportation

Please remember: If there is any spare room in the Cash Carrying Case, it is preferable to place stock in the case rather than the inconspicuous carrying bag.

- Return all equipment used (eg, Horizon, etc) to your vehicle first and lock it in the boot
- Then take the inconspicuous carrying bag to your vehicle and lock it in the boot
- Finally take the Cash Carrying Case and place it in your vehicle, ideally in the passenger footwell or behind the front seats

POL00423229

- Lock the car doors before setting off.

Please note: These procedures apply to any additional Outreach site that you visit in the course of one day's sessions.

On your return to the 'Core' branch

- Park as near to the entrance of the 'Core' branch as possible
- Check the surroundings to ensure that there are no suspicious circumstances before you unload your vehicle
- Remove the Cash Carrying Case first and take it straight into the secure area of the 'Core' branch, locking the door behind you
- Then remove the inconspicuous carrying bag from the boot of the vehicle and return it to the secure area of the 'Core' branch
- Remove the cash and other secure items from the Cash Carrying Case and lock them in the safe
- Remove any additional stock or coin from the inconspicuous carrying bag and lock them in the safe

Please note: If, in exceptional circumstances, the time overlock on the main safe has been activated by the time you return to the 'Core' branch, the cash can be stored in the Cash Carrying Case overnight, as long as it is in the secure position.

- Then remove the other items of equipment from the boot of your vehicle and store them as instructed.

Collecting surplus cash and stock (Partner branches only)

If you are collecting cash and stock using the Cash Carrying Case:

- Ensure the access doors at the Partner site are locked and clear of unauthorised personnel at the time of collection.
- Lock the cash and secure stock in the Cash Carrying Case.

In all instances:

- Secure the key used to open the case in a lockable drawer/cupboard at the Partner site.

Integrity of mail

Mail items must be always be regarded as items of security, in keeping with the policy for mails integrity (see para 8.1; page 24).

To ensure the security of mail, mail items that you accept must always be kept in the Post Office controlled environment, ie, behind the counter or desk and not available for customers to see or reach. Special Delivery items must be kept in a lockable drawer or the Cash Carrying Case. Whenever possible, Special Delivery items should be transported in the Cash Carrying Case.

Carrying out transactions

Completion of transactions

Transactions must be completed as quickly as possible: cash, secure stock and documents must be secured in the lockable drawer straightaway. Cash and documents, and the stamp folio must always be kept in the lockable drawer and not be left on top of the serving area.

Transactions up to the value of £600 only can be accepted at the serving area. Cash must be deposited in the counter drawer as soon as possible and transferred to the Cash Carrying Case as soon as the site is clear of customers.

Confidential information must not be left in a position where customers can read it.

Security of cash and stock, documents, etc, using the lockable drawer

Extra care must be taken in safeguarding cash and stock, etc, while you are carrying out transactions in a screen-less environment.

POL00423229

A lockable drawer (with slam-shut lock) must be used to store the cash float, the stock including the stamp folio, and the datestamp. these items must not be left on top of the serving area. The lockable drawer at the serving position must be closed immediately after use, and locked whenever you leave the serving position, regardless of the length of absence. Keys to counter drawers must not be kept in the locks at any time.

There should never be £600 at risk at any one time in the drawer at the serving position. Any cash exceeding this must be stored in the Cash Carrying Case.Replenishment of the cash from the Cash Carrying Case must always be carried out discreetly.

All holdings of licences and other secure stock items must be kept to the minimum level to meet the requirements of providing an efficient service to the public, and must be kept in the lockable drawer. Obtaining further supplies during the day would be preferable to over-stocking. At the close of business Motor Vehicle Licence discs, the datestamp, etc, must be secured in the Cash Carrying Case for secure transportation to the next Outreach site or to the 'Core' branch. If there is not enough space in the Cash Carrying Case, the datestamp and the stamp folio may be carried in the inconspicuous bag. Alternatively, the stamp folio may be stored in the lockable drawer as long as the value of the stamps does not exceed £600.

Transactions over £600

You may carry out transactions up to a limit of £600.

Arrangements for the acceptance of Alliance & Leicester deposits, or payments to a customer, of over £600 must be made in advance between the sub postmaster and the customer. The premises must be cleared of customers and the doors locked for the duration of the transaction.

Procedure at the close of business

At the close of business the normal practice is to remove all cash and secure stock items including the stamp folio and Motor Vehicle Licences, and datestamp from the counter drawer and to place them in the Cash Carrying Case, ready for return to the 'Core' branch. However, if necessary, the lockable drawer can be used as secure overnight storage for the stamp folio and coin up to a maximum value of £600.

POL00423229

31 Index

POL00423229

POL00423229

Index