Cyber Security Standards

Acceptable Use Standard

Version – V2.2

1 Overview

1.1 Introduction by the Standard Owner

Post Office is committed to protecting its employees, customers, Third Party Supply Chain and information assets from damaging or illegal actions by individuals, either knowingly or unknowingly. Post Office enables this through the development and deployment of policies, standards and guidelines which are aligned to international best practices. Effective cyber and information security is a team effort involving everyone in Post Office.

1.2 Purpose

The Acceptable Use Standard defines a set of business rules governing fair and acceptable use of Post Office's information assets.

Every Employee has a responsibility to understand the requirements set out in this policy, if there is any misunderstanding, the employee must gain clarification from their line manager.

1.3 Core Principles

Compliance with this standard will ensure that the following principles are met:

- Both individuals and Post Office are better protected from any legal action;
- Email correspondence with third-parties has acceptable content, is appropriately secured and the necessary levels of confidentiality are maintained;
- Post Office's IT systems perform optimally for their intended use;
- Post Office email system is used in a way that provides a cost effective and efficient form of communication; and
- Post Office maintains high standards as set out in guidance such as Post Office Business Standards.

1.4 Application

This standard applies to all Post Office staff and Third-Party organisation's who have access to Post Office data especially those with elevated rights to Post Office data.

This Access Control Standard is amended from time to time, and applies to all Post Office staff, including third party suppliers providing services to, for, or on behalf of Post Office, and aligns to the requirements of the Cyber and Information Security Policy.

.

2 Policy Framework

2.1 Policy Framework

This standard forms part of the Cyber and Information Security Policy Set. This contains controls that form part of the Information Technology Control Framework (ITCF) governed by the overarching Post Office wide framework.

2.2 Who must comply?

Compliance with this standard is mandatory for all Post Office employees and applies wherever in the world Post Offices business is undertaken. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this standard or have their own equivalent policy/standard.

3 Minimum Controls

The table below sets out the minimum control standards.

Control Ref	Control Objective	Control Guidelines
PHT0940	Assign ownership of the information security program to the appropriate role.	Assign the responsibility for establishing, implementing, and maintaining the information security program to the appropriate role. Assign information security responsibilities to interested personnel and affected parties in the information security program. Assign the responsibility for distributing the information security program to the appropriate role. Disseminate and communicate the information security policy to interested personnel and affected parties.
PHT0945 CTRL0020506	Establish, implement, and maintain operational control procedures.	Establish, implement, and maintain a Standard Operating Procedures Manual. Disseminate and communicate the Standard Operating Procedures Manual to all interested personnel and affected parties. Include that explicit management authorization must be given for the use of all technologies and their documentation in the Acceptable Use Policy. User Access Management all colleagues must • Choose strong passwords • Never share User IDs / passwords

Control Ref	Control Objective	Control Guidelines
		• Report any suspected Misuse to the Service Desk, or to IT Security. • Never displaying passwords in clear text on any device. • Remove all sensitive information from screens when taking support calls where remote access is instigated. • Ensure that remote connections have been closed when the support call • Change their password if they suspect it has been compromised. The Access Control standard can be found. • Remember that User ID's and passwords are confidential, and must only be used for sanctioned activities and/or communications • All Colleagues must be aware that all actions taken with their allocated User ID are their responsibility. • Third Party Suppliers shall assert that their own Acceptable Use Policy (or equivalent) has the same requirements. All colleagues are required to follow physical security controls: • Wear their physical passes at all times whilst on • Post Office premises. • Challenge anyone who does not display a pass • if they feel safe to do so take an escorted visitor who does not have their host with them back to reception.

Control Ref	Control Objective	Control Guidelines
		• Third Party Suppliers whose staff have a Post Office pass are required to ensure their employees are aware of this requirement. They will assert that this occurs annually • You have a responsibility to promptly report the theft, loss or unauthorised disclosure of Post Office proprietary information. • Post Office requires colleagues and Third Party Providers report information security incidents or suspected information's security incidents to information.security GRO • If the incident concerned includes personal data, then this must be reported to the data.protection GRO mailbox. • Third Party Suppliers are expected to adhere to the Cyber Security Incident Response Team standard (CSIRT), and assert their compliance annually. • IT has built functionality into the Digital Service Desk portal which allows users to post outage notifications, which can be found under Service Status.
PHT0950	Include requiring users to protect restricted data in accordance with the Governance, Risk, and Compliance framework in the Acceptable Use Policy.	When working away from Post Office premises: • Take care that they are not overlooked when working on confidential or strictly confidential information. • Not use public internet connections (e.g. Cafes, airports, public hotspots) to connect to Post Office services, unless expressly authorised to so and via VPN.

Control Ref	Control Objective	Control Guidelines
		• Always use the provided software to connect to Post Office when using trusted Wi-Fi. • Connect to Post Office via VPN only. If VPN is not always an applicable option, then use it as often as possible to receive latest software updates and security patches. Alternately you must visit the main office and connect your devices to the network via cable. • Never initiate a scan for devices when attaching to a public Wi-Fi - this is a question that often gets asked, just click No. • Third Party Suppliers who attach to Post Office networks must have equivalent controls in place and assert that these are in place annually Social Media all colleagues must: • Only publish Post Office information to social media sites if authorised to do so. • Be aware of the information you post online on social media as you not have the ability to remove it in the future. • Never publish confidential, strictly confidential information or legal privilege information. Using corporate systems safely all colleagues must • Not access inappropriate or illegal sites. • Not change settings to lower security controls. • Not post confidential, strictly confidential information or legal privilege information.

Control Ref	Control Objective	Control Guidelines
		• Not Copy, screenshot, or photograph confidential or strictly confidential information (e.g. PAN). • Not store cardholder data (full card number) unless it's absolutely necessary. • Not store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones. Take care when saving confidential or strictly confidential data in SharePoint or Teams who has permission to view this information. • You may access, use or share Post Office proprietary information only to the extent it is authorised and necessary to fulfil your assigned job duties. • Service Providers must assert that they have equivalent requirements in place annually. All colleagues must protect data by operating safely when browsing the internet: • Think before they click. • Not access inappropriate or illegal sites. • Not change browser settings to lower security controls. • Not store large amount so personal information on Post Office equipment. • Not store any business related personal data on corporate systems such as servers. • Not use social media outside Post Office guidelines.

Control Ref	Control Objective	Control Guidelines
		• Not post confidential, strictly confidential or legal privilege information to the public internet. • Must not access illegal or unauthorised file sharing services (this includes but is not limited to: Dropbox, SkyDrive and iCloud) unless authorised to do so for legitimate business purposes. • Service Providers must assert that they have equivalent requirements in place annually All Colleagues must protect the data by operating safely when using e-mail: • Not send information that violates laws, or regulations. • Not send confidential or strictly confidential information via insecure methods (email, IM etc.). • Not send unsolicited commercial announcements or advertising material unless approved by management beforehand. • Not send any material that may defame, libel, abuse, embarrass, or portray the recipient or Post Office in a false light. • Not use your corporate e-mail address for non –work related activities (shopping apps etc.). • Third Party Suppliers must assert annually that they have equivalent requirements.
PHT0951	Include asset tags in the Acceptable Use Policy.	All colleagues must: • Adhere to the information classification standard found. • Post Office proprietary information stored on electronic and computing devices whether

Control Ref	Control Objective	Control Guidelines
		owned or leased by Post Office, the employee or a third party, remains the sole property of Post Office. You must ensure through legal or technical means that proprietary information is protected. For devices not owned by the Post Office you can also refer to the BYOD standard. • Clear your desk when away for significant periods of time, and at the end of the day. • Report Lost Equipment to the Service Desk. • Lock screen when moving away from the desk (⊞ + L). • If your job involves working on confidential or strictly confidential information, ensure you have a privacy screen in place.
PHT0952	Include asset use policies in the Acceptable Use Policy.	Include authority for access authorization lists for assets in all relevant Acceptable Use Policies. Include access control mechanisms in the Acceptable Use Policy. Include temporary activation of remote access technologies for third parties in the Acceptable Use Policy. Include prohibiting, copying, or moving of restricted data from its original source onto local hard drives or removable storage media in the Acceptable Use Policy. Expectation of Privacy:

Control Ref	Control Objective	Control Guidelines
		• All colleagues must be aware that all actions taken using their User IDs is being logged and audited, and in certain situations could be monitored. • For security and network maintenance purposes, authorised individuals within Post Office may monitor equipment, systems and network traffic at any time. • Further details are in the Monitoring Section of this standard.
PHT0957	Correlate the Acceptable Use Policy with the network security policy.	Include appropriate network locations for each technology in the Acceptable Use Policy. Correlate the Acceptable Use Policy with the approved product list.
PHT0960	Include a software installation policy in the Acceptable Use Policy.	All Colleagues must protect Post Office from fines for misuse of software: • Comply with software licences • Not download and install software, e.g. gaming apps on their work phone, health guides, etc.. • Third Party Suppliers must assert that they have equivalent requirements within one of their own policies on an annual basis
PHT0961	Document idle session termination and logout for remote access technologies in the Acceptable Use Policy.	Have a defined disconnection time for session termination. No users should have unlimited access.
PHT0962	Disseminate and communicate the Acceptable Use Policy to all interested personnel and affected parties.	Establish, implement, and maintain an Intellectual Property Right program. All colleagues are not authorised to pass statements to the press unless they are given permission by the

Control Ref	Control Objective	Control Guidelines
		communications department to do so. All requests for contact must be passed to the press office via pressoffice GRO. Further details of actions prohibited are covered under the Unacceptable Use section of this document.
PHT0964	Establish, implement, and maintain Intellectual Property Rights protection procedures.	All colleagues must: • Pass any requests from customers or colleagues for information to the information rights team foiteam GRO • Report anything suspicious to the service desk, Grapevine or Cyber Security immediately. • Third Party suppliers must also ensure they have processes in place to pass requests onto the Post Office information rights team and assert the existence of such annually.

4 Monitoring

Post Office staff with access to our systems is could be provided with an email account, Skype for Business access, Teams access, SharePoint/OneDrive access, as well as access to the internet to carry out their Post Office business.

Everyone using these facilities must comply with Post Office policies, and the UK law that applies. These are:

- Post Office's monitoring of communications in transit must comply with the Investigatory Powers Act 2016 The detailed provisions are specified in The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- When the email, skype conversations, Teams conversations, Zoom calls, Chime, WebEx, etc. or internet browsing have reached the end user's machine, The Acceptable Use Standard states that Post Office systems will be audited and monitored to ensure proper usage of the system. All colleagues should be aware that the system is provided for business purposes, so under the Data Protection Act 2018 users should not expect privacy.

4.1 Email

The End User Computing (EUC) Service provider are responsible for the management of the email service. The Service Desk run by Post Office also have some access to the Exchange system. The Cyber Security, Data Protection and the Information Rights teams also have access to the mail system in order to satisfy P6 requests.

The email system is used for internal and external communication, and can be used to send attachments. Any attachments form part of the email, and in this document, it includes any attachments.

4.2 Alteration, blocking or deletion of emails in transit or after delivery for Post Office protection

Post Office operates a number of mechanisms to protect Post Office colleagues, including those to prevent the introduction and spread of viruses, and for the prevention of harmful code reaching Post Office from the Internet. Emails can be deleted or amended in transit for the following reasons:

- If the email has come from outside Post Office, or an email is being sent to outside from within Post Office and has as an attachment a file with a format (egg VB Script) which is not permitted.
- If the email from outside contains a program (e.g .exe extension) file. In these cases the email minus attachment is delivered, and a message informs the recipient their email and/or attachment has not been sent or delivered and how to proceed.
- If the spam detection system has detected that an email is classed as spam or those that have a virus detected within them it will be held in quarantine and not reach the recipient's inbox. Legitimate emails may also be quarantined. This is unfortunate, but necessary for the overall protection of Post Office.

4.3 Data Leakage Protection

To comply with business standards and industry regulations, Post Office must protect sensitive information and prevent its inadvertent disclosure. Sensitive information can include, but not limited to, financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. Post Office have a Data Loss Prevention (DLP) solution in place that will identify, monitor, and automatically protect sensitive information across the Post Office estate.

4.4 Reading another person's emails

There are certain users of the email system who allow others to access and read their emails. The permissions which have been granted by the user can be seen by clicking on the name on the email and looking at the members. However, there are occasions when emails have to be read by other parties. To read *delivered* emails in another person's mailbox for which permissions have not been granted by the owner, a P6 request must be made by the manager of the person who's mailbox is to be investigated, or an individual senior to the person's manager, detailing why access is being requested, or a security alert has been triggered. No lower delegated authority is acceptable.

The types of reasons why read access may be permitted are:

- To prevent *or* detect crime e.g. fraud, corruption
- To investigate or detect unauthorised *use* e.g. breach Post Office's rules on the use of email and the internet such as the sending of abusive emails, or their conditions of employment such as the sending of sensitive or confidential information to the press
- To establish the existence of facts which are relevant to our business e.g. keeping records of transactions and other communications where specific facts are required, particularly with contractual obligations
- To answer an information request under the Freedom of Information Act or Data Protection Act.

In order for the EUC service provider, the Information Rights team, Data Protection Team, or the Cyber Security team to read the emails in an account or grant permission to another person on an email account, they can only do so, if authorised as a result of the P6 process or an external request via the Freedom of Information Act or the Data Protection Act.

4.5 Clearing down unused accounts / mailboxes.

Mailboxes may be accessed prior to deletion in order to confirm whether they are still in use. The EUC Service Provider use indicators to flag up apparently dormant mailboxes and the associated Logon ID. These indicators include:

- Mailbox not being accessed for 90 days
- Associated Logon ID not being accessed 90 days

These dormant mailboxes are then marked for deletion.

4.6 Information on Team sites, SharePoint and OneDrive

As for email, there are circumstances when information on these storage systems, may need to be accessed. Examples of these are:

As part of the implementation of our Data Loss Prevention software, searches for specific types of information, such as personal or Payment Card information, are searched for by accessing all files in the systems named above. The Cyber Security team have access to assess the risk to Post Office and will work with users to mitigate that risk.

If illegal or offensive material is found, the presence will be logged with HR. Depending on the location of the material, the ensuing investigation will involve the owner of the One Drive or the owners of the other systems being searched to find out who is responsible for the placement of the material.

As for email there are other reasons as to why Team sites, SharePoint or OneDrive may be investigated:

- To prevent or detect crime e.g. fraud, corruption
- To investigate or detect unauthorised use for instance to ensure that employees do not breach Post Office's rules on the use of Post Office in respect of the data they are storing on the named systems.
- To establish the existence of facts which are relevant to our business egg keeping records of transactions and other communications where the specific facts are required, particularly with contractual obligations.
- To answer an information request under the Freedom of Information Act or Data Protection Act.

4.7 Internet

The EUC service provider, and the Security Operations team provide the boundary security services for Post Office, including all firewalls to Post Office network and all onward connections. Their primary functions are the protection of Post Office internal services from the Internet; the operation of the firewalls. The Post Office SOC monitors Post Office firewalls MON-FRI 8:00 – 18:00 (excluding Bank Holidays) for attempts of 'hacking', and excessive traffic on the firewall. No further authorisation is required for any work completed by the named teams, as all investigations are triggered by security alerts.

All internet traffic must go via proxy, the proxy should never be bypassed.

4.8 Monitoring Logs

Post Office logs all activity through all the security systems in place around our perimeter. Internet usage is monitored through the Post Office proxy. The logs would tell the Information Security team which sites a person had accessed. These are only accessed through the P6 process or as a result of a security alert.

5 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that hos t is disrupting production services).

Under no circumstances is an employee of Post Office authorised to engage in any activity that is illegal under local, state, federal or international law while utilising Post Office owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

5.1 System and Network Activities

The following activities are strictly prohibited:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Post Office.
- Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Post Office or the end user does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting Post Office business, even if you have authorised access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a Post Office computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Post Office account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee

is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- Port scanning or security scanning is expressly prohibited unless prior notification to the Cyber Security team is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Introducing honeypots, honeynets, or similar technology on the Post Office network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Post Office employees to parties outside Post Office.

5.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realise they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

Questions may be addressed to the IT Department

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorised use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Post Office’s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Post Office or connected via Post Office’s network.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.3 Blogging and Social Media

- Blogging by employees, whether using Post Office's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Post Office's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Post Office's policy, is not detrimental to Post Office's best interests, and does not interfere with an employee's regular work duties. Blogging from Post Office's systems is also subject to monitoring.
- Post Office's Information Classification Standard also applies to blogging. As such, Employees are prohibited from revealing any Post Office confidential or proprietary information, trade secrets.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Post Office and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging.
- Employees may also not attribute personal statements, opinions or beliefs to Post Office when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Post Office. Employees assume any and all risk associated with blogging.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Post Office's trademarks, logos and any other Post Office intellectual property may also not be used in connection with any blogging activity, unless agreed with the Group Head of Communication.

6 Where to go for help

6.1 Additional Policies

This standard is part of the Cyber Security Policy framework. The full set can be found at:

https://poluk.sharepoint.com/sites/cybersecurity2/SitePages/Cyber-and-Information-Security-Policy-Set.aspx

6.2 How to raise a concern

Any Post Office employee who suspects something is wrong has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by contacting the IT Helpdesk

6.3 Who to contact for more information

If you need further information about this standard or wish to report an issue in relation to this standard, please contact Cyber Security Team via cyber@postoffice.co.uk.

7 Version Control & Approval

7.1 Version Control

Date	Version	Updated by	Change Details
18/12/2019	0.1	Cyber Security	Initial draft of the acceptable use standard
30/03/2020	0.2	Cyber Security	Updated to meet the Deloitte audit requirement
12/06/2020	1.0	Cyber Security	Approved by ISC
13/05/2021	1.1	Cyber Compliance	Updated minimum controls to include PCI-DSS restrictions
25/06/2021	1.2	Cyber Compliance	Updated to cover questions by employees and organisational restructuring
28/07/2021	1.3	Cyber Compliance	Final approval version
02/08/2021	2.0	Cyber Compliance	Approved version
10/04/2023	2.1	Cyber Compliance	Update the controls to align with the UCF.
25/04/2023	2.2	Cyber Compliance	CSF approval for publication

7.2 Standard Approval

Standard Owner:	Chief Information Security Officer
Standard Author:	Ehtsham Ali
Approved by CSF:	25/04/2023
Next review:	25/04/2024