Parliamentary
and Health Service
Ombudsman

Acceptable Use Policy

V2.2 | May 2021

If you would like this document in a different format such as Daisy or large print, please contact us

Policy objectives

This acceptable use policy provides clarity on what you can and cannot do with information, networks and systems provided by PHSO. This is to protect everyone, both staff and complainants, by keeping our information safe and reducing the risk of inadvertent or malicious misuse.

What is new in this version?

- From October 2020, PHSO staff can use Microsoft Teams to communicate with each other, complainants, external advisors, and others.
- PHSO staff can also join video conferences organised by others using Zoom or WebEx. However, staff must treat these calls as public and must not share personal or sensitive information.

Policy scope

This policy applies to people, information, and things;

- Everybody who works in or with PHSO including staff, consultants, contractors, clinical and expert advisors, and companies operating on our behalf that have access to PHSO information assets and systems.
- Every item of information we have including when it is stored as physically for example as paper, on dictation machines, fire exit signs, CDs, USB drives, payslips, Dictaphones, cameras, and medical evidence. These are all information assets.
- Everything that we use to manage, connect, or view our information including email, internet, telephones, smartphones and tablets, systems and software, Wi-Fi, and videoconferencing.

Policy statements

Good information management is efficient, effective, and respectful of the privacy of our staff, complainants, and others. When we get things wrong, people whose information may be compromised could suffer distress and harm. PHSO is also exposed to the risk of reputational, financial, and regulatory penalties.

This policy set out what is and is not acceptable use of PHSO information and technology. In doing so we aim to reduce information risks. The restrictions described in this policy are proportionate and pragmatic.

Most information handled by PHSO identifies or is about people. This personal data must be treated with care. Examples include using encrypted email to send information to complainants or making sure the locations of paper records are recorded in our systems.

We ensure the effectiveness of these arrangements by monitoring information systems access and use, including email and voicemail to ensure compliance with this policy.

Any employee found to have not complied with any of the requirements of this Acceptable Use Policy may be subject to disciplinary action. If any contractor or third party user is found to have not complied with any of the requirements of this Acceptable Use Policy, PHSO will take such steps as are necessary to remedy the position including termination of engagement, action to secure restitution or formal escalation to the contractor's or third party user's organisation.

Acceptable use of computers and information systems

Access to PHSO information is controlled by checking that someone has the right to access information before being let into our network. Users can be asked for who they are (their username), something they know (their password) and something they have (e.g. entering a code generated on a device that they possess). This third level of authentication is known as two factor and is mandatory for remote and mobile access. Away from the office or on mobile device, staff will be asked to re-authenticate on a frequent basis.

All the above are unique to individuals and can be used to identify who has done what when.

PHSO information systems and related resources must not be used to download, process, store or transmit any material that could be offensive or derogatory.

Acceptable use of video-calling tools

PHSO recognises the benefit of using videoconferencing tools such as Microsoft Teams to collaborate and continue to work as a team even when each team member is working remotely.

Microsoft Teams brings people together in a virtual workplace. Just like in the office, PHSO's code of conduct continues to apply. PHSO will not tolerate any offensive or derogatory behaviour.

Microsoft Teams must not be used to download, process, store or transmit any material that could be offensive or derogatory.

All Teams meetings, whether video, audio or through the chat function are private and secure. However, Teams creates a record of each meeting. This does not include the detail of the conversation, but who were the participants and how long it lasted. If the meeting organiser attached documents, then those documents would be retained as part of the meeting record. If the chat function is used, then comments made and reactions e.g. 'likes' will also be recorded. This record is retained by PHSO for a period of one year which is the same as email and outlook calendar appointments.

Microsoft Teams can be used for:

- Meeting with colleagues virtually using video and audio as appropriate
- Conversing with other meeting participants using the chat function.
- Sharing screens so that all participants are looking at the same information.
- Telling your colleagues where you are and whether you are busy (presence management)
- Talking with complainants, clinical advisors and other third parties.

When using Microsoft Teams:

- Users shall only connect to Microsoft Teams via PHSO's global connect solution which provides a virtual private network (VPN). This ensures that your Microsoft Teams conversations are encrypted and secured.

- Users shall not download files received via Microsoft Teams to their desktop computer outside of the VMWare Horizon Client (VDI). If they do so in error, users shall delete immediately.
- Users shall not install software without authorisation from ICT.

Before using videoconferencing tools, users must;

- Make sure that there is a fallback option e.g. telephone call, in case the call does not work as expected. This is important particularly when it comes to meeting with complainants as issues may occur due to their home network or connections which are beyond PHSO's control.
- Learn how to mute their microphone and how to turn off the camera before joining the call.
- Many video-conferencing services including Teams allow participants and organisers to record the meeting, share files, or show what is on somebody's screen. PHSO does not allow staff to record meetings. However, meetings which have been set up by a third party, may be recorded and this is beyond PHSO's control. For this reason, all externally organised videocalls must be treated as 'public'. Users must ensure that they know how to tell if a meeting is being recorded. If in doubt, contact the HelpHub for advice.
- If participants know that a conversation is being recorded and may later be shared more widely, this may have an impact on what they do and say. If a member of PHSO staff does not wish to be recorded, then inform the meeting organiser in the first instance. If the meeting organiser continues to record the meeting, PHSO staff members can switch off their video or microphone or otherwise withdraw politely from the meeting. If a PHSO staff member is concerned that their privacy has been compromised, please contact the data protection officer. Ensure that any external meeting participants are provided with private links (as described in the Using Microsoft Teams Guidance). This is to ensure that Microsoft Teams meetings are not hi-jacked by a third party.
- Make sure people are who they say they are before they join the call by using the lobby feature for external parties.

On a call, users shall;

- Think about what your camera shows when you are on a call.

- Ensure that information in their background is appropriate to display in the call. If not, remove or blur or change the background

Microsoft Teams is PHSO’s default video-calling option and should be used by PHSO when arranging or initiating video-calls. However, there will be times when a third-party arranges a meeting via an alternate such as Zoom or Webex. PHSO staff can participate in these calls if the following criteria are met:

- Users should access Zoom, Webex or other collaborative application through a browser. Users must not attempt to download and install software to their device.
- Users shall assume that their meeting is not secure and conduct themselves with care. Users must not discuss personal information unless the privacy of the call has been verified by information security.
- Learn how to mute their microphone and how to turn off the camera before joining the call.
- Many video-conferencing services allow participants and organisers to record the meeting, share files, or show what is on somebody's screen. Users must ensure that they know how to tell if a meeting is being recorded. If in doubt, contact the HelpHub for advice.

Acceptable use of video recording

Video recording can be controversial as people may behave differently or express concerns about their image being recorded. However, there are some circumstances where recording is necessary. These are summarised below.

Requirement 1 | Events, Communication and Training:

- Where PHSO staff whose job involves organising and running events, communication and training at which, it would be reasonable for attendees to expect to be recorded. This includes:
- Learning and development staff for whom recording their workshops will enable greater participation for example, those who were unable to attend.
- □ Communications and public affairs staff who facilitate or organise public or partnership meetings when transcripts and recordings can further promote inclusivity and accessibility.

- Staff involved in creating podcasts or other broadcast materials for publication.
- Internal communications staff capturing corporate messaging.

Requirement 2 | Governance and Executive Officer purposes:

- Where office staff who use recordings and/or transcripts of meetings to ensure the accuracy and timeliness of minutes and records of decision making.
- These recordings and/or transcripts are created solely for this purpose and should be deleted promptly after the meetings have been documented and, in all cases, no later than 5 working days following the meeting.

Requirement 3 | By exception:

- Where there are other business justifications for recording video, not included in either requirement 1 or 2 above.
- These requirements will be managed by exception with a formal email request submitted for review and approval or rejection in the first instance to the ICT HelpHub.

Acceptable use of mobile devices

Users of PHSO issued mobile devices, including laptops, mobiles and iPad must comply with the requirements below detailing how they are to be accessed, used, stored, and protected.

- Mobile devices will be protected by secure authentication which comply with the PHSO Password Policy. This includes password, PINs, codes, and biometrics where appropriate.
- Immediately report actual or suspected loss, theft, or misuse to security@ombudsman.org.uk
- Users shall update their mobile device when prompted by the device or instructed by ICT.
- Users shall not plug in their personal mobile devices to PHSO's office network unless specifically authorised to do so.
- Users can make reasonable use of PHSO's issued devices for personal communications and entertainment when travelling. For further advice please discuss with your line manager.

When laptops and mobile devices are taken out of the office, users shall:

- Use a virtual private network (VPN) to connect to PHSO's network
- Do not connect to untrusted networks such as cafes, hotels etc.
- Act in accord with the PHSO remote working policy;
- Not leave laptops and mobile devices unattended in public places or vehicles;
- Carry laptops and mobile devices as hand luggage when travelling.
- Protect your passwords and screens from nosey or intrusive people.
- Protect mobile devices and laptops with a strong password (see PHSO password policy)
- Not connect a PHSO laptop or mobile device to another by Bluetooth, NFC, or other potentially insecure solution. This includes tethering (using a mobile phone signal to connect to the internet).
- Keep information on mobile devices, including laptops, Dictaphones, mobile and ipads to a minimum to reduce our risk in event of loss, theft, misuse, or damage.

Do not install apps that are not on the PHSO approved app list. For queries or to add an app not featured, please submit a request though Helphub. Do not attempt to install a non-approved app.

If saving documents, save to PHSO's sharepoint or one drive. Only save information to a mobile device if it can be encrypted using software installed by IT. This applies to all mobile devices including Dictaphones, cameras, and other recording devices.

If a PHSO mobile device is lost, stolen or damaged the user must report this immediately to the Information Security Manager ++security@ombudsman.org.uk or call the ICT Help Hub on 0300 061 4100 (Extn. 4100)

Acceptable use of internet and email systems

PHSO internet, applications and email are provided for staff to do their jobs. Limited personal use is permitted but will be monitored. Staff should not use email or the internet in such a way that it impacts on their productivity or causes harm to PHSO or others.

Staff are permitted to make reasonable and appropriate personal use of web shopping and banking services. However, PHSO does not guarantee the safety of your financial details or other personal information. Other examples of reasonable use could include browsing the web on your lunch break or checking your train times. If in doubt, discuss with your line manager.

PHSO’s internet and email systems must not be used for;

- Running your own business in PHSO’s time or using PHSO’s resources to do so (for example, buying and selling on eBay, or posting influencer videos)
- Sending offensive messages
- Harassment or vexatious behaviour (e.g. trolling or cyber bullying)

Acceptable use of your own device

PHSO's standard policy is to provide staff with a secured device or computer managed by the ICTY department. However, in emergencies or during a business continuity incident, using your own device is possible but only under certain conditions. This is to ensure that allowing people to use their own machines does not compromise our security.

Personal laptops can be connected to PHSO’s network to work remotely only when the following criteria are met:

- Access to your device is controlled by a strong password.
- Access to your device is locked if an incorrect password is input too many times.
- Your device is set to lock automatically if inactive for a period.
- Your device runs either Microsoft Windows 10 or Mac OS operating systems.

- You have installed the software required to access PHSO’s network as instructed by ICT prior to logging into PHSO’s network from your own device.
- You immediately inform PHSO security if you suspect your device is infected with a virus, lost, or otherwise compromised.
- You separate business and personal use for example by not using your device to work and to access music streaming services at the same time.

- You must not use your laptop to connect to public Wi-Fi such as that provided by cafes, coffee shop and hotels whilst using your laptop for PHSO work.
- You must not take screenshots or photographs of PHSO information.
- You have appropriate security measures installed and up to date on your device including anti-virus. These must be maintained.
- You either lock your device or close a remote session when away from the device such as going to make a cup of tea. Be extra vigilant with children.
- You do not allow your children or others in your household to play with the device during an active network session.
- You understand that your use will be monitored.
- You have changed the default password on your laptop
- You must not connect any other devices such as mobile telephones, external storage devices (such as USB memory sticks, CDs) and tablets to your laptop during a PHSO remote working session. This includes using your mobile phone to connect to the internet (tethering).

If you have any questions or concerns, please contact the Help Hub 0300 061 4100 (Extn. 4100) or email ICT-Support-PHSO@live.hornbill.com

To report a security breach, please email security@ombudsman.org.uk

Acceptable use of CDs, USBs, Dictaphones, and cameras

Before using these peripherals, consider whether the business need to do so outweighs the privacy and security risks. If unsure, raise a call with the Help Hub.

Personal data including photographs, videos interview recordings must only be saved to encrypted devices. If it is impossible to encrypt, then the peripheral device must be treated with care and caution. Whilst in storage these peripherals must be held in a secure and locked cabinet. In transit, these devices should be only sent by secure courier and their contents (records such as interview recordings, photographs) logged on the appropriate system.

Any data transfer from a peripheral (Dictaphone, camera etc needs to be actioned by ICT services within a safe environment. The device must then be securely wiped.

If you are expecting to receive large files on CD, such as medical records, log a call with the Help Hub (who can check for malicious code and then upload to our systems, once verified.)

Acceptable use of telephones

PHSO telephones and faxes are provided for work purposes however a reasonable number of personal calls will be permitted. PHSO will routinely monitor telephone usage. If in doubt, discuss with your line manager.

Unacceptable use of mobile devices and technology

You must not use web solutions to save information to or use your own device to work unless through the 'use your own device' solution approved by PHSO. This includes accessing office and outlook solutions through a web browser.

You must not make unauthorised changes to the security settings of any PHSO device

Policy Information

Author: Angharad Jackson

Related policies and guidance: Employee Privacy Notice

Version control

Date	Version	Content/changes made	Owner of changes
13/10/2020	2	Updated to reflect Teams deployment	Angharad Jackson
14/10/2020	2.1	Changes to monitoring of video calling, definition of offensive or derogatory behaviour	Angharad Jackson, Gill Kilpatrick
08/4/2021	2.2	Added policy position on video recording	Angharad Jackson

If you would like this document in a different format such as Daisy or large print, please contact us