

Public Service

Ombudsman

Acceptable Use Policy

V4.2 | February 2025

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

1 Policy objectives

1.1 What is new in this version?

- Clarity regarding the use of your Public Service Ombudsman email and restrictions on the automated forwarding rule to external email address.

Policy scope

This policy applies to people, information, and everything we use.

- Everybody who works in or with us including staff, consultants, contractors, clinical and expert advisors, and companies operating on our behalf that have access to our 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.

2 Policy statements

- 2.1 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. We are also exposed to the risk of reputational, financial, and regulatory penalties.

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

3 Acceptable use of computers and information

- 3.1 Access to our 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
- 3.2 All the above are unique to individuals and can be used to identify who has done what and when.
- 3.3 Our information systems and related resources must not be used to download, process, store or transmit any material that could be offensive or derogatory.

4 Acceptable use of video-calling tools

- 4.1 We recognise 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.

- 4.2 Microsoft Teams brings people together in a virtual workplace. Just like in the office, our code of conduct continues to apply. We will not tolerate any offensive or derogatory behaviour.
- 4.3 Microsoft Teams must not be used to download, process, store or transmit any material that could be offensive or derogatory.
- 4.4 All Teams meetings and activities, whether video, audio or through the chat function and team sites are private and secure. However, Teams creates a record of each meeting and interaction. 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 us for 3 months and for chat withing a channel will be a 12-month period.
- 4.5 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 not install any software without authorisation from ICT.
- Users must be logged into multi-factor authentication as directed by us.
- User should only access using a corporate device e.g., laptop, iPad, or iPhone.

4.6 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 our 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. We only allow staff to record meetings in specific circumstances as detailed in the Casework Call Recording Policy. However, meetings which have been set up by a third party, may be recorded and this is beyond our 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 our 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, our staff members can switch off their video or microphone or otherwise withdraw politely from the meeting. If a staff member is concerned that their privacy has been compromised, please contact the Data Protection Officer (DPO).
- 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.

- Be aware of your surroundings and where possible always try to find a private space to conduct meetings. When in the office always be aware of what can be heard around you. If you are not speaking use the mute option to avoid picking up background noise. Especially within the office as when seated at your desk it may not be obvious to those around you that you are on a call or where possible make people aware you have to take a meeting.
- 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 our default video-calling option and should be used by staff 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. 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 should access Zoom, Webex or other collaborative application through a browser. Users must not attempt to download and install software to their device.
- 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.

5 Acceptable use of video recording

- 5.1 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.

5.2 Requirement 1 | Events, Communication and Training:

Where our 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.

5.3 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 | Reasonable adjustments

- 5.4 Some colleagues will benefit from being able to record and transcribe meetings to support them in their duties. This is always acceptable and will be permitted. As with all recordings, all participants must be made aware prior to recording starting. However, should a member of staff not agree to be recorded they are welcome to withdraw from the meeting or switch their video off.
- 5.5 Where there are other business justifications for recording video, not included in either requirement 1, 2 or 3 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.

6 Acceptable use mobile devices

- 6.1 Users of Public Services Ombudsman 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 Password Policy. This includes password, PINs, codes, and biometrics where appropriate.

- Immediately report actual or suspected loss, theft, or misuse to via helphub.
- 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 the office network unless specifically authorised to do so.
- Users can make reasonable use of Public Service Ombudsman issued devices for personal communications and entertainment when travelling. For further advice please discuss with your line manager, this will be monitored by DSP

- 6.2 When staff are working outside the office they must:

- Not leave laptops and mobile devices unattended in public places or vehicles.

- If in a public space avoid connecting to public wifi where possible, this is to prevent information from becoming compromised by insecure wifi networks. If possible, creating a hotspot from your phone will be more secure. If Gov wifi is available you can use your work email to connect and use this service.
- Always consider your surroundings especially when in public look for an area with some privacy. Where possible work with your back to a wall or in a booth space to avoid people being able to see your screen from behind you.
- Ensure you lock your screen or minimise documents/data displayed on your screen when not actively working on them.
- Carry laptops and mobile devices as hand luggage when travelling.
- Protect your passwords and screens from nosey or intrusive people.
- Use a privacy screen where possible to secure their desktop from view by others in the vicinity.
- Protect mobile devices and laptops with a strong password (see our password policy)
- 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 our approved app list (Company Portal). 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 sharepoint or one drive. Only save information to a mobile device if it can be encrypted using software installed by IT.

7 Acceptable use of internet and email system

- 7.1 Our 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 the Public Service Ombudsman or others.
- 7.2 Staff are permitted to make reasonable and appropriate personal use of web shopping and banking services. However, we cannot guarantee the safety of your financial details or other personal information.
- 7.3 Public Service Ombudsman does not permit the use of your work email address to sign up to non-work-related sites and services. And prohibits the use of the automated forwarding rule for emails from your work account to an external email account.
- 7.4 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.
- 7.5 Public Service Ombudsman's internet and email systems must not be used for.
- Running your own business during work hours or using our 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)

8 Acceptable use of CD's, USBs, Dictaphones, and cameras

- 8.1 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.
- 8.2 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.
- 8.3 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.
- 8.4 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.)

9 Acceptable use of web-based apps or service

- 9.1 There are a lot of free or low-cost web solutions for collaboration, sharing information, project management and presentations now available. Whilst these tools may be alluring in terms of the services they provide, generally they make their money through acting as data brokers. This means selling information at scale on to global buyers. There may also be other privacy and security concerns. We will monitor use of unauthorised apps on a regular basis so if you are using an web tool or app and haven't received authorisation, your access is likely to be revoked. Before you start to use a web app or service, you must log a call with HelpHub to gain access otherwise you risk losing your work and exposing us to privacy, security, and reputational risks

10 Unacceptable use of mobile devices and technology

- 10.1 You must not use web solutions to save information to or use your own device to work. This includes accessing office, outlook solutions and third-party applications through a web browser.
- 10.2 You must not make unauthorised changes to the security settings of any Public Service Ombudsman device.

11 Policy information

Author: Angharad Jackson

Related policies and guidance:

- Employee Privacy Notice
- Casework Call Recording Policy

Version control

Date	Version	Amends	Owner of amends
------	---------	--------	-----------------

13 Oct 2020	2	Updated to reflect Teams deployment	Angharad Jackson
14 Oct 2020	2.1	Changes to monitoring of video calling, definition of offensive or derogatory behaviour	Angharad Jackson, Gill Kilpatrick
1 March 2023	3	Review to update the AUP to reflect security updates and general changes.	Nada Leddy Rouse
19 Jan 2024	4	Update to point defining more guidance about working outside of the office.	Nada Leddy Rouse
28 Feb 2025	4.1	Added clarity to section 7 regarding use of our email and restrictions on use of the automated forwarding rule	Nada Leddy Rouse
6 March 2025		Review complete no update needed	UU
18 Sep 2026	4.2	Rebrand amendments	Charlotte Carter