ICT Acceptable Use Policy

Purpose and Scope

1. This policy provides guidance for staff and managers on acceptable use of PHSO ICT systems and how these are controlled and monitored.

2. This includes guidance on what is considered appropriate personal use of our systems, and the responsibilities of staff members for the maintenance of their accounts.

3. The policy applies to all PHSO ICT devices and systems, including PCs and laptops, telephones, email, internet access, the PHSO internal network, BlackBerry devices, iPhones and iPads, and mobile phones.

4. The policy applies to all staff, permanent or otherwise, temporary agency staff and any contractors who have access to PHSO ICT facilities.

Principles

5. PHSO provides an ICT infrastructure for official use and some permitted personal use. The ICT systems must not be used in any way that damages them, breaks the law, causes offence to colleagues, exposes our information to unnecessary risk, or harms PHSO's reputation.

6. Access to internal ICT systems will be continuously monitored. A log will be kept of users' actions on the PHSO network, including logging in and out, activity on our information systems, web access and email use.

7. PHSO has no objection to staff making reasonable and appropriate personal use of our ICT systems, within the boundaries defined by this policy. Line managers must judge what is reasonable and appropriate, but excessive or other use which impacts on performance is not acceptable.

8. The IT Security Officer will keep this policy under review in consultation with the Security & Information Assurance Committee and Leadership Team.

Objectives

9. All employees and contractors have a clear understanding of their personal and collective responsibilities in using ICT systems provided for the Office.

10. Appropriate monitoring and control arrangements are in place to ensure that information is safeguarded and systems are not used inappropriately.

11. Security of our information is maintained, and our responsibilities in the PSN Code of Connection and PHSO Protective Marking Scheme are fulfilled.

Version History	
Date agreed	**Agreed by**
11/01/11	Executive Board (meeting)
07/02/12	Executive Board (circulation)
23/04/13	Leadership Team (circulation)
07/10/14	Executive Team (circulation)

1 ICT and information security

1.1 All staff (and contractors where appropriate) must agree to abide by this policy before being permitted to use PHSO's ICT systems. This is arranged through inductions for staff and the distribution of the policy as appropriate. Agreement to abide by this policy is explicitly requested as part of the login process to all PHSO computers.

1.2 Contact the Head of ICT if you have any queries or concerns about IT security. Contact the Head of IRM if you have any queries or concerns about information security or personal data.

2 Passwords

2.1 Never share your network password with anyone. Never write down your network password or record it in an electronic file or email.

2.2 If you forget your password , the ICT Helpdesk can provide you with a new one. If someone else needs to access your account, the Head of ICT and the Director of HR, People & Talent can authorise the ICT Helpdesk to provide them with controlled access.

3 Locking your machine

3.1 In order to reduce the risk of your account being misused, you should lock your machine when you leave it unattended. In case you forget, it will lock automatically after 5 minutes of inactivity, but your account will be vulnerable during that time. Turn your computer and monitor off when not in use. This saves electricity as well as improving security.

4 Optical discs, Peripherals and USB devices

4.1 Some PHSO computers are equipped with optical drives for reading CDs and DVDs. Where this is not the case, ICT staff will be able to assist you.

4.2 Do not attempt to read a disc that has come from a source from which you were not expecting to receive information in this format. The ICT Helpdesk can help you scan a disc for viruses and other malware.

4.3 Optical discs are small and therefore easily misplaced or concealed, but they have a large capacity and can hold a significant amount of personal or sensitive data. The loss or disclosure of such data could involve PHSO in considerable expense and embarrassment.

4.4 To limit our exposure to these risks, staff are not permitted to write to CDs or DVDs; contact the ICT Helpdesk if you need to write information to a disc. Be sure to exercise due care when transporting a disc outside PHSO premises, see the Security Guidance for further details on handling arrangements for electronic information.

4.5 Similar risks are introduced by the use of USB-enabled devices, such as memory sticks and music players. Only devices owned by PHSO may be connected to our computers. USB ports have been disabled for data transfer on all PHSO computers; contact the ICT Helpdesk if you need to write to or read information on a USB device.

5 Remote access

5.1 Remote access to PHSO systems is granted via a thin client laptop or mobile device (BlackBerry, iPad or iPhone). These devices are covered by dedicated Security Operating Procedures (SyOPs).

5.2 Where users require changes to a computer to make it accessible to meet specific needs, the ICT Helpdesk will undertake customisation of the remote access equipment, as appropriate.

6 Data ports

6.1 All wall and floor ports are administered by Facilities and should not be interfered with. Do not unplug any wall or floor ports that are in use, and do not connect any device to a vacant wall port without consulting Facilities.

7 Software

7.1 The software installed on your machine has all been tested for stability and security, and is licensed and administered by the ICT team.

7.2 Do not install any extra software on your machine, either from the internet or by installing it from a CD or other medium. This extends to any licensed software already owned by PHSO, which must only be installed by ICT staff.

8 Your Windows desktop

8.1 Store documents in Meridio, not on your desktop. Each desktop has a very small size, and if you exceed this you will be unable to log out of your machine. Also, desktops are not included in our nightly backups so any corruption to a computer could result in lost work. The desktop should only be used for shortcuts, or to temporarily hold documents before saving to Meridio.

9 Email management

9.1 Refer to the Records Management Policy for the principles of email management in PHSO. Further guidance on how to effectively manage emails and when to save them as PHSO records is given during induction IRM training and on the IRM guidance pages on the intranet.

9.2 In the case of planned absences (e.g. holidays) staff should set up an Automatic Reply, giving an alternative contact and stating when a full reply can be expected. In the case of unplanned absences and/or where the member of staff has not made arrangements for access (e.g. sickness) the manager should arrange setting up an Automatic Reply; authorisation should be requested from the Head of ICT.

9.3 There may be occasions when it is necessary to access email messages from an individual's mailbox when a person is away from the office. Authorisation should be requested from the Head of ICT and the Director of HR, People & Talent. Access should be in the presence of the line manager. On return, the staff member should be told when and why their mailbox was accessed. The reasons for accessing an individual's mailbox are to action:

- Subject access request under the Data Protection Act;
- Freedom of Information request;

- Evidence in legal proceedings;
- Evidence in a criminal investigation;
- Line of business enquiry; and
- Evidence in support of disciplinary action.

10 Copyright

10.1 When managing electronic information, copyright legislation must be respected. If you have any doubts or queries consult the Legal Team. Infringement of copyright is a serious matter and could involve PHSO in considerable expense and embarrassment. Specifically:

- Carefully consider copyright when downloading information from the internet that you plan to reuse, especially if this involves disseminating it outside PHSO;
- The content of emails must not be in breach of copyright;
- You must consider copyright when photocopying or scanning material;
- Do not copy software from your machine. If you have any queries regarding the installation or licensing of software, contact the ICT Helpdesk.

11 Email content, social media and legal liability

11.1 PHSO is legally liable for the content of emails and social media comments from PHSO accounts, just as it is for the content of letters. Despite the informal, conversational writing style common in email and social media, you should apply the same professional standards that you would apply to a letter on PHSO letterhead, particularly when writing to third parties and representing PHSO.

11.2 The content of emails should not be defamatory or in breach of PHSO's Dignity at Work or Equality and Diversity policies. Emails can be treated as a permanent record and could be used in court proceedings. Specifically:

- Do not make statements that could be interpreted as the official PHSO position, or committing PHSO, unless authorised and intending to do so;
- Obtain the same authorisation to send an email as you would for a letter;
- Ensure information provided is accurate;
- Do not use poor spelling or grammar in messages, particularly to other organisations;
- Avoid defamatory statements, rumours, and gossip about individuals, organisations or companies;
- Only transmit personal data if PHSO's Protective Marking Scheme and Security Guidance permit. If in doubt, contact the Head of IRM;
- Get clearance from Media, Marketing and Internal Communications before issuing any message that amounts to a press release.

12 Personal use of Social Media

12.1 PHSO recognises that members of staff use social media channels such as Twitter, LinkedIn and Facebook in a personal capacity. While they are not acting on behalf of PHSO, staff must be aware that they can cause damage to our reputation if they are recognised as being one of our employees.

12.2 If you state that you work for PHSO, ensure that your name or the title of your profile does not contain ‘PHSO’ or ‘Parliamentary and Health Service Ombudsman’, and include on your profile a statement such as: “The views that I express here are mine alone and do not necessary reflect the views of my employer.” Generally, and in addition to the guidelines for email above:

- Refrain from making statements that compromise your impartiality;
- Do not criticise or argue with colleagues, customers, or stakeholders or do anything that could bring PHSO into disrepute;
- Do not post images that are inappropriate or links to inappropriate content;
- Do not reveal confidential information about the work of PHSO or discuss its internal organisation;
- Do not share information you would not want a journalist to see.

13 Personal use of the ICT system

13.1 All ICT systems are PHSO property and are intended for business use. However, PHSO has no objection to staff making reasonable and appropriate personal use of our systems, including web browsing, telephony and email. It will be for line managers to judge what is reasonable and appropriate, but excessive or other use which impacts on performance is clearly unacceptable.

13.2 Responsible personal use of our ICT systems is permitted, provided that it:

- does not interfere with job performance;
- is not for commercial or business gain;
- does not contravene any of PHSO’s policies and guidelines;
- is not detrimental to PHSO in any way.

13.3 Staff may not use personal web-based email services, such as Gmail or Hotmail. These present a threat to the security of PHSO’s network and data, and are blocked from within the PHSO network.

13.4 Staff may not use their personal logins on social networking sites, such as Facebook and Twitter. However, staff are permitted to access the PHSO Facebook and Twitter pages, which are maintained by the Media, Marketing and Internal Communications team. Access to LinkedIn is also permitted.

13.5 Discussion forums may be used for work purposes, but it is important that any conversation resulting in a decision needs to be recorded in Meridio; therefore official electronic correspondence should all be conducted through PHSO’s email system.

13.6 Do not use your PHSO email address to subscribe to any email list, forum, shop or other online service which is not work-related.

13.7 Except where required for business purposes, accessing streaming media sites such as YouTube is not permitted. This is to prevent the downloading of large video and audio files, which can have an impact on network performance.

13.8 Non-networked internet computers and wireless internet access are available for personal use in Millbank Tower and The Exchange. Where users require changes to a computer to make it accessible to meet specific needs, the ICT Helpdesk will undertake customisation of the non-networked internet computers, or offer an alternative method of access, as appropriate.

13.9 PHSO permits staff to make reasonable and appropriate personal use of web shopping and banking services. However, PHSO does not and cannot guarantee the safety of your financial details or other personal information.

14 Unacceptable use of the ICT system

14.1 All of the following types of activities are strictly prohibited and are subject to normal disciplinary procedures. This list is not exhaustive:

- Unauthorised attempts to circumvent any of PHSO's electronic security or monitoring systems;
- Unauthorised attempts to access another user's account;
- Unauthorised attempts to read, delete, copy, or modify documents or data on the network;
- Unauthorised attempts to read, delete, copy, or modify the email of other users;
- Forgery (or attempted forgery) of email messages;
- Sending emails that are harassing, obscene, offensive, illegal or threatening;
- Sending unsolicited junk email, 'for-profit' messages or chain letters.

14.2 Staff should not access online material which is related to:

- sexual content;
- discrimination/hate;
- illegal activities;
- circumventing electronic or computer security;
- violence;
- gambling.

14.3 The deliberate access of inappropriate material is a serious disciplinary offence, and sites falling in to those categories should be blocked by PHSO systems. If you accidentally visit an inappropriate site, please notify the Head of ICT promptly so that this can be taken into account in monitoring the logs of sites visited.

14.4 PHSO may decide to block particular websites at any time, without giving prior notice, if it considers it appropriate to do so. If access to a blocked website is required for business reasons, this can be arranged by contacting the ICT Helpdesk.

15 System monitoring

15.1 PHSO ICT systems will be continuously monitored. These logs are necessary for system administrators in the event of technical problems, as well as providing a record for auditing or in the event of misconduct.

15.2 Activities that are logged include:

- logging on and off the network;
- accessing or modifying data in Meridio;
- accessing or modifying data on Visualfiles;
- printing documents;
- use of email;

- internet access.

16 Email monitoring

16.1 PHSO monitors email use. System administrators are able to read or access emails and will grant access to other staff if authorised by the Head of ICT and Director of HR, People & Talent. The Head of ICT has the authority to suspend any email account believed to have been inappropriately used.

16.2 Managers may request information on a staff member's email use from ICT if they have a concern about unreasonable or inappropriate use. The request will be authorised by the Head of ICT and Director of HR, People & Talent.

16.3 If you receive 'spam' (unsolicited email), contact the ICT Helpdesk and the address will be blocked where possible. PHSO may block email from domains or addresses at any time if it considers it appropriate to do so.

17 Web monitoring

17.1 Web access is continuously monitored; this includes secure connections, including https. A log is kept of all web use and this will be audited regularly.

17.2 If web monitoring reveals a cause for concern about inappropriate use the Head of ICT will discuss with the Director of HR, People & Talent whether further investigation is appropriate.

17.3 Managers may request information on a staff member's web use from ICT if they have a concern about unreasonable or inappropriate use. The request will be authorised by the Head of ICT and Director of HR, People & Talent.

18 Hardware inspections

18.1 ICT staff may examine any PHSO ICT equipment in order to confirm that it is being used in accordance with this policy.

19 Disciplinary action

19.1 Misuse of PHSO's ICT systems is regarded as misconduct. All investigations into misuse will be conducted according to PHSO's policies concerning Discipline, Grievance, Dignity at Work and Forensic Readiness, which may result in action being taken and could ultimately lead to dismissal.