IT Acceptable Use Policy

Mandatory Policy

The Institution of Engineering and Technology
Futures Place
Kings Way
Stevenage
Hertfordshire
SG1 2UA

IT Acceptable Use Policy

1. Why we have this Policy

1.1 This document outlines the IET policy and procedure regarding the acceptable use of equipment and services provided by the IT & Digital Services Directorate in order for you to be able to carry out your role.

1.2 The policy seeks to ensure that all employees, volunteers, contractors, and temporary staff understand their responsibilities with regard to IET equipment and services and provides direction to ensure standards are harmonised, fair, and consistent.

2. Who this Policy relates to

2.1. The Acceptable Use Policy applies to all employees, volunteers, contractors, and temporary staff (where they have been supplied access to IET IT services or systems). For the purposes of this document the term “staff” will be used to refer to all persons within scope.

2.2. All staff are required at all times to comply with the IET’s Acceptable Use Policy. All users are contractually responsible for ensuring that they have read this policy and complete all mandatory data protection and security training.

2.3. Any staff found to have acted or be acting in contrary to this policy may be subject to action under the Disciplinary, Suspension and Appeals Policies. Volunteers found to have acted or be acting contrary to this policy may be subject to action under the Disciplinary Regulations.

3. Other Policies, Procedures and/or Guidelines you need to read in relation to this Policy

3.1. Disciplinary, Appeals and Suspension Policies

3.2. Disciplinary Regulations

3.3. Driving on Company Business policy

3.4. Display Screen Equipment Assessments

3.5. Information Security Policy

3.6. Data Protection Policy

3.7. Information Classification Policy and Retention Schedule

3.8. Third Party Data Protection and Security Due Diligence Risk Procedure

3.9. Personal Information Risk Management Procedure

3.10. Password Guidance

4. Overview of this Policy

4.1. The IET is the legal owner of the systems and services provided to you in order to carry out your duties whilst on IET business. The IET retains the right to monitor and view usage, access, unencrypted & encrypted content, and any other files created, stored, sent, or received using any IET provided system. This access is undertaken for the purposes of security, regulatory or legal compliance maintenance and disciplinary purposes.

4.2. All staff are responsible for exercising good judgment regarding appropriate use of IET resources in accordance with all relevant IET policies, procedures, standards, and guidelines. IET resources may not be used for any unlawful or prohibited purpose; for example, but not limited to:

4.2.1. Accessing the IET's, or another organisation's services/systems for which you are not authorised.

4.2.2. Causing intentional disruption to either an IET, or another's, service(s) or intentionally introducing viruses, spyware, or any form of malware.

4.2.3. Breaching any statutory or regulatory requirements as laid out in relevant law, such as the UK GDPR or Computer Misuse Act.

4.2.4. Violating copyright law or international technology embargoes.

4.2.5. Publishing information or content of a defamatory, bullying, sexually explicit nature, that is likely to incite racial hatred or damage the reputation of the IET.

4.2.6. Excessive use for non-work related activities.

4.2.7. Engaging in commercial activities that do not relate to IET business.

4.3. The use of personal devices (mobile phones, tablets, laptops, smart speakers etc) to access IET systems is prohibited. Access to IET systems should only be undertaken using IET approved equipment, unless operating under approved exception.

4.4. Please be aware that other systems or services that you may use during the course of your work may employ their own Acceptable Use Policies which must be adhered to and taken as supplementary to this policy.

5. Service Access and Password/Account Management

5.1. Staff are provided with access to IET systems that are relevant to their role. If you require access to additional systems raise an IT Service Centre ticket outlining the reason for the access. Authorisation will be sought from your line manager and the owner of the system before access is granted. Where varying levels of access to systems are available, you will only be provided with the level necessary and relevant to your role.

5.2. Staff are accountable for actions completed using their login credentials. Your computer must be locked whenever you are away from your desk to help prevent unauthorised access to IET systems and data.

5.3. Staff are responsible for creating, keeping confidential and using appropriate passwords for accessing IET systems and services. Passwords must meet the criteria set out in the "Password Guidance" document referenced in section 3.

5.4. Never share a password with anyone, including managers, directors, system administrators, personal assistants etc. All passwords are to be treated as confidential IET information. It is unacceptable to provide your password to a colleague who is covering your work during holidays and other absences; no one should ever ask you for, nor should you ever divulge, your password(s)

5.5. If you suspect that your login or any password has been compromised, you must change your password immediately and report this to the IT Service Centre without delay.

5.6. Try to create passwords that are sufficiently complex to avoid being guessed, but which are memorable to you. For example, take a phrase that has special meaning to you and take the first letter of each word. You can then add numbers and special characters to make the password more secure. Alternatively use three completely random words. Passwords should never be written down or stored on-line in an easily readable format. The use of “password manager” applications and apps are permitted. For further information please refer to the “Password Guidance” document referenced in Section 3.

5.7. Do not re-use IET account passwords on non-IET systems (e.g. personal Webmail, social media sites etc).

5.8. Never re-use passwords.

5.9. Should you forget your password or for some reason require it to be reset, please contact the IT Service Centre for assistance.

5.10. Managers are responsible for being familiar with and following the relevant Joiner, Movers & Leavers processes. If you are unsure, please contact the IT Service Centre.

6. Email

6.1. It is a disciplinary offence to access another individual’s e-mail mailbox without their permission unless the IET is required to comply with an obligation under the law. In exceptional circumstances, managers should seek the advice of their HR Business Partner if access is required. All reasonable measures should be taken to keep information confidential where appropriate.

6.2. If it is apparent that a message or file sent to an employee was intended for someone else, the file should be closed immediately, the message and/or file deleted, and the sender advised that it was mis-addressed and has been deleted.

6.3. Do not send or forward e-mails known to contain viruses or malware (either internally or externally). Use the Report Message in Outlook if you believe the email or attachment to be a threat, junk or spam.

6.4. Any, sensitive, personal or confidential data sent by e-mail must be first encrypted, any queries regarding this should be directed to the Data Protection Officer.

6.5. Bear in mind that if you make reference to or record information relating to any individual whether in an e-mail, document, or other format this may be disclosed to the individual concerned via a Subject Access Request as per the UK GDPR.

6.6. Requests for additional e-mail mailboxes should be submitted through the IT Service Centre.

7. Internet

7.1. Access to the Internet is provided in order that you can carry out your duties within the IET. Limited personal (non-work related) use is permitted as long as it does not interfere with your duties, does not interfere with other people carrying out their duties and provided that the use does not contravene other sections of this policy.

7.2. No software or upgrades of any sort are to be downloaded from Internet sites without permission from the IT department.

7.3. No software or services should be purchased or subscribed to without prior authorisation from the IT department. Authorisation and approval will be

via the IT Service Centre.

7.4. Under no circumstances must IET IT facilities be used for illegal activity or for downloading offensive, obscene or indecent material. Where such activity is accidental or in the normal course of work, you should make your line manager aware.

7.5. The IET employs web filtering systems for the purposes of protection against harmful / illegal / prohibited content with blocked web addresses being logged. The logs of this service may be reviewed as per section 4.1 of this policy.

8. Wi-Fi

8.1. The IET may, in its various buildings, provide Wi-Fi networks for the convenience of staff and visitors.

8.2. Staff Wi-Fi - Only IET-owned equipment and devices may be connected and will be setup by IT staff. Personal devices and guest equipment must not be connected to this network.

8.3. Guest Wi-Fi - where provided, is intended only for visitors to the IET's buildings who require internet access. They will need to enter a username and password (obtained from Reception) and agree to terms and conditions, presented at the Wi-Fi login page before use.

8.4. BYOD Wi-Fi - “Bring Your Own Device” where provided for the convenience of staff, is intended for the connection of personally-owned devices for limited personal use. The connection key is provided through the Noticeboard on the Intranet, please contact the IT Department ifyou are unable to locate the key.

8.5. Under no circumstances should the key for a BYOD Wi-Fi network be given to someone who is not a member of IET staff, nor access to guest networks provided to someone other than a legitimate visitor to one of the IET's buildings.

8.6. This policy applies to the use of any device (mobile, tablet, laptop, etc), including personally owned devices, connected to any IET supplied Wi-Fi connection.

9. PC, Laptops & Printers

9.1. The IT Service Centre will provide a standard desktop or laptop with the relevant software required for your role. This approach allows quick swapping of faulty hardware and minimises problems for users resulting from custom configurations. Where additional software or a non-standard desktop/laptop is required, managers should discuss options with the IT department. No hardware, software or IT services should be procured or installed without necessary manager and IT approval.

9.2. IT department will maintain appropriate backups of systems and servers including L drive and OneDrive - local disk drives on desktops and laptops (e.g. C: drive) are not backedup and should not be used

9.3. The IT Service Centre is responsible for the decommissioning and removal of IET supplied equipment and uses fully accredited secure disposal services, please do not dispose of IET supplied IT equipment yourself. Managers are responsible for being familiar with and following the relevant Joiner, Movers & Leavers processes. If you are unsure, please contact the IT Service Centre.

9.4. IET devices (laptops, desktops, tablets, and mobile phones) are provided for business purposes. Some limited personal use is allowed subject to the monitoring controls outlined in Section 4.1. Please be aware that security and monitoring technologies are in use on approved IET devices for the purposes of protecting the

organisation'sinformation assets and regulatory compliance.

9.5. No software or hardware should be installed or procured without the prior authorisation of the IT Department, who will ensure that appropriate licences are held, and relevant security assurances are undertaken.

9.6. The IET will provide training and support for users of IT systems where appropriate. It is the responsibility of all staff to seek training and advice for any software or facility with which they are unfamiliar, or where questions arise.

9.7. Workstations and other IT equipment may not be transferred between users without the IT Service Centre being informed. This is to ensure our asset register is updated and data security / protection.

9.8. The IT Service Centre will provide all workstations with access / login controls and virus protection. Under no circumstances should users interfere or attempt to interfere with their normal operation.

9.9. No attempt should be made to by-pass or disable any security features installed on IET equipment.

9.10. PCs and laptops should be shut down when not in use for extended periods; this will not only save power, but regular restarts also help to ensure that software updates are applied.

9.11. Devices must be locked whenever they are left unattended to help protect against unauthorised access.

9.12. All staff should complete a DSE (Display Screen Equipment) self-evaluation and home workers should also complete a Home Workplace Environment Assessment. For further details please contact HR.

9.13. Please remember that data security procedures also apply to printed data. Do not print documents unnecessarily and ensure that printed documents containing sensitive information are shredded or put into the IET confidential waste bins after they have been used. Any printing found unattended should be disposed of in confidential waste bins or shredded.

9.14. The provision of printers within the IET is for business related printing and should not be used for personal printing.

10. Portable Storage

10.1. Portable storage devices refer to USB memory sticks and Mass Storage Devices, smart phones, and other devices capable of acting as storage devices when connected to computers.

10.2. All staff must consider the additional risk of loss or theft posed by portable storage devices holding IET data.

10.3. Only encrypted devices which have been supplied by the IT Service Centre should be used.

10.4. If a device is lost or stolen, this must be reported immediately to your line manager and to the IT Service Centre.

10.5. Where a portable storage device is known to be carrying a virus, then under no circumstances must it be connected to any IET equipment.

10.6. When you connect a portable storage device, the IET's anti-virus software will scan the drive. Under no circumstances should the virus scan be interrupted or bypassed.

10.7. If a virus or malware risk is identified during this scan, then you must call the IT Service Centre immediately.

11. Cloud Storage

11.1. The IET provides all staff with access to a range of internal services to store data (L Drive, OneDrive etc).

11.2. The IET also provides cloud-based services for certain corporate data storage and processing (e.g. Inspec, CRM, Microsoft 365) which are provided and supported by the IT Department and have been assessed from functional, security and reliability perspectives.

11.3. If you have a business requirement to use an alternative cloud storage service, this should be discussed and agreed with your line manager. Log a service centre ticket and the Information Security team and the Privacy Office will follow the Third Party Data protection and Security Due Diligence Procedure.

12. Mobile Devices

12.1. Mobile devices (phones, tablets) will be provided to users whose current job specification requires such equipment, or on a temporary loan basis as required. Please consult your line manager in the first instance.

12.2. Mobile devices are provided by the IET for business purposes. An IET company app store is provided for a wide range of applications. Limited personal use is permitted, provided that this does not contravene other sections of this policy and does not interfere with the performance of your legitimate duties, those of your colleagues or put at risk IET systems or data. If in doubt, then permission should be obtained from your line manager. As per section 4.1, please be aware that mobile devices are subject to the same monitoring controls as other IET devices.

12.3. The IET reserves the right to monitor mobile phone usage, and where unacceptable levels of personal usage are presented, also reserves the right to investigate.

12.4. Use of mobile devices in vehicles is subject to the policy on Driving on Company Business policy and any relevant local law.

12.5. Mobile devices must be returned to the IT department when no longer required or when staff leave. Managers are responsible for ensuring compliance with this requirement.

12.6. A pool of tablet devices is available for temporary loan purposes. Requests should be made to the IT Service Centre.

12.7. In cases of loss, theft, or unauthorised access please contact the IT Service Centre so the device can be remotely disabled and/or wiped. Please also contact your line manager.

13. Purchasing & Licensing

13.1. All software and hardware must be security assessed, approved and purchased through the IT department. Requests for software and hardware should be made through the IT Service Centre. This includes purchase or subscriptions of cloud-based services. In addition any proposed arrangements with third parties that involve access or sharing of IET personal data must be security assessed and approved by IT.

13.2. Staff will submit a Service Centre ticket and the Third Party Security and Data

Protection Due – Diligence Risk Procedure will be followed. Staff will be expected to cooperate by providing all relevant information and complete a Data Protection Impact Assessment (DPIA) if required, in order to support risk assessment and implementation of any necessary security mechanisms needed to protect the personal data the supplier will have access to.

13.3. The IET reserves the right to review all software installed on its devices, to ensure that it is licensed correctly for business purposes. All IET devices are subject to audit. Action may be taken where devices are found to be non-compliant.

13.4. IET licensed software must not be installed on personally owned, home or other non-IET equipment. Where software is required for carrying out work-related activity using such hardware, written permission for its installation must be obtained from the Head of IT Services or Director of IT and Digital Services.

13.5. These guidelines apply equally to IET desktop computers, laptops, and any other hardware.

14. IT Security Incidents

14.1. Avoid unnecessary risks to your workstation and therefore to IET systems, such as downloading or opening files or messages or clicking on links that you are not expecting, and of whose origins you are uncertain.

14.2. Risks are not limited to being “computer based”. Be aware of people, especially those you do not know, asking for your logon details or for you to send information which they should not really be asking for.

14.3. If you feel that you have been the victim of a virus attack or any other form of security or social engineering breach, you must:

14.3.1. Call the IT Service Centre immediately informing them of the situation and follow any and all instructions they give you; and

14.3.2. Contact the Privacy Office as soon as possible if the incident is not cyber related or if the incident involves IET personal information. privacyoffice@theiet.org Tel: (0)7808 102171

14.3.3. Not send any emails, access any files, folders, or servers until a member of the IT Services team has investigated the issue.

14.3.4. Do not forward any emails on, report using the Report Message button in Outlook

14.3.5. Shutdown and disconnect any potentially infected devices in order to limit spread.

14.4. As appropriate the IET Cyber Attack Response Plan will be followed.

14.5. As appropriate the IET Incident and Data Breach Management Plan should be followed.

15. What happens if you do not follow this Policy

15.1. Any staff found to have acted or be acting in contrary to this policy may be subject to action under the Disciplinary, Suspension and Appeals Policies. Volunteers found to have acted or be acting contrary to this policy may be subject to action under the Disciplinary Regulations.

16. Queries and Comments

16.1. If you have any queries regarding how this Policy works in practice, or comments or suggestions as to how it could be improved, please contact the Information Security Group.

Appendix

Control Sheet

Click here to enter document name Policy

Sponsor:	Information Security Group
Document reviewer:	Information Security Group
Document adopted on:	**1 January 2016**
Next review date:	**May 2023**

Review/change history

Date of Review/Change	Summary of changes	Version no.
11/08/2014	New document, rationalisation, and consolidation of previous disparate IT policies	0.1
04/11/2014	Inclusion of comments and feedback on version 0.1	0.2
01/12/2014	Final review and minor amendments for submission to Executive	1.0
6/1/2016	Annual Review and Update, improving clarity, risk based approach for cloud storage, clarity on use of Guest Wi-Fi	1.1
22/8/2016	Reference to web filtering included minor tidy up	1.2
26/08/2016	Updates to Cloud Storage section and minor tidy up	1.3
19/09/2016	Updates to Password/Account Management	1.4
15/02/2017	Annual Review	1.5
28/02/2018	Annual Review	1.6
26/07/2019	Annual Review	1.7
19/02/2021	Annual Review	1.8
24/05/2022	Updates to include Third Party Security and Data Protection Due Diligence Procedure	1.9