# IET Policy

## Category of Policy
IT

## Policy Name
IT Acceptable Use Policy

<table>
<thead>
<tr>
<th>Effective date</th>
<th>Approved by</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2016</td>
<td>Executive Committee</td>
<td>IT Security Group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date of last review</th>
<th>Reviewed by</th>
<th>Date of next review</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2016</td>
<td>IT Security Group</td>
<td>January 2017</td>
</tr>
<tr>
<td>January 2016</td>
<td>IET General Counsel</td>
<td>January 2017</td>
</tr>
<tr>
<td>January 2016</td>
<td>Data Protection Officer</td>
<td>January 2017</td>
</tr>
<tr>
<td>February 2017</td>
<td>IT Security Group</td>
<td>January 2018</td>
</tr>
<tr>
<td>February 2018</td>
<td>IT Security Group</td>
<td>January 2019</td>
</tr>
<tr>
<td>July 2019</td>
<td>IT Security Group</td>
<td>July 2020</td>
</tr>
</tbody>
</table>

**Distribution:** All Staff (via Intranet)

## Change History

<table>
<thead>
<tr>
<th>Version</th>
<th>Author</th>
<th>Date</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>N Day</td>
<td>11/08/2014</td>
<td>New document, rationalisation and consolidation of previous disparate IT policies</td>
</tr>
<tr>
<td>0.2</td>
<td>N Day</td>
<td>04/11/2014</td>
<td>Inclusion of comments and feedback on version 0.1</td>
</tr>
<tr>
<td>1.0</td>
<td>N Day</td>
<td>01/12/2014</td>
<td>Final review and minor amendments for submission to Executive</td>
</tr>
<tr>
<td>1.1</td>
<td>N Day</td>
<td>06/01/2016</td>
<td>Annual Review and Update, improving clarity, risk based approach for cloud storage, clarity on use of Guest Wi-Fi</td>
</tr>
<tr>
<td>1.2</td>
<td>N Day</td>
<td>22/08/2016</td>
<td>Reference to web filtering included, minor tidy up</td>
</tr>
<tr>
<td>1.3</td>
<td>N Day</td>
<td>26/08/2016</td>
<td>Updates to Cloud Storage section and minor tidy up</td>
</tr>
<tr>
<td>1.4</td>
<td>N Day</td>
<td>19/09/2016</td>
<td>Updates to Password/Account Management</td>
</tr>
<tr>
<td>1.5</td>
<td>N Day</td>
<td>15/02/2017</td>
<td>Annual Review</td>
</tr>
<tr>
<td>1.6</td>
<td>T Unger / R Best</td>
<td>28/02/2018</td>
<td>Annual Review</td>
</tr>
<tr>
<td>1.7</td>
<td>R Best</td>
<td>26/07/2019</td>
<td>Annual review</td>
</tr>
</tbody>
</table>
# Contents

1. Purpose ...........................................................................................................................................3
2. Scope ...............................................................................................................................................3
3. General ...........................................................................................................................................3
4. Service Access and Password/Account Management .................................................................4
5. Email ..............................................................................................................................................4
6. Internet ...........................................................................................................................................5
7. WiFi ................................................................................................................................................5
8. PCs, Laptops & Printers ................................................................................................................6
9. Portable storage .............................................................................................................................6
11. Mobile Devices ............................................................................................................................7
12. Purchasing and Licensing ...........................................................................................................8
13. IT Security Incidents .....................................................................................................................8
14. Related Policies and Procedures ................................................................................................8
1. **Purpose**
   
   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 in regards to IET equipment and services and provides direction to ensure standards are harmonised, fair and consistent.

2. **Scope**

   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.

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

   2.4 See section 14 for a list of policies, procedures and guidance which should be read in conjunction with this policy.

3. **General**

   3.1 The IET is the owner of the systems and services which are provided to you solely in order that you can carry out your duties within the IET and therefore retains the right to monitor/view usage, access, unencrypted & encrypted content and any other files created, stored, sent or received using any IET provided system or service for the purposes of security, regulatory or legal compliance maintenance and disciplinary purposes.

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

   3.2.1 Accessing the IET’s, or another’s, services/systems for which you are not authorised;

   3.2.2 Causing intentional disruption to either an IET, or another’s, service(s) or intentionally introducing viruses, spyware or any form of malware;

   3.2.3 Breaching any statutory or regulatory requirements such as the Data Protection Act;

   3.2.4 Violating copyright law or international technology embargoes;

   3.2.5 Publishing information or content of a defamatory, bullying, sexual explicit nature, that is likely to incite racial hatred or damage the reputation of the IET;

   3.2.6 Excessive use for non-work related activities;
3.2.7 Engaging in commercial activities that do not relate to IET business.

3.3 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.

4. Service Access and Password/Account Management

4.1 Staff are provided with access to IET systems that are relevant to their role. If you require access to additional systems raise a helpdesk service 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.

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

4.3 Staff are responsible for creating, keeping confidential and using passwords for accessing IET systems and services. Passwords must meet the criteria set out in the “Password Guidance” document referenced in section 14.

4.4 Do not share IET passwords with anyone, including managers, directors, system administrators, personal assistants etc. All passwords are to be treated as confidential IET information. It is not acceptable to provide your password to a colleague who is covering your work during holidays and other absences; no one ever should ask you for your password(s).

4.5 If you suspect that your login or password has been compromised, change your password and report the concern immediately to the IT Service Centre and follow any additional instructions they may give you.

4.6 Try to create passwords that you can remember. 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. 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 14.

4.7 Do not use the same password for IET accounts as for other non-IET access (e.g. personal Webmail, social media sites etc).

4.8 Where possible, do not use the same password for multiple IET systems.

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

5. Email

5.1 It is a disciplinary offence to access another individual’s e-mail facility without their express permission except in emergencies, where managers should seek the advice of their HR Business Partner. All reasonable measures should be taken to keep information confidential where appropriate.

5.2 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 miss-addressed and has been deleted.
5.3 Do not send e-mails known to contain viruses or malware (either internally or externally).

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

5.5 Bear in mind that if you refer to any individual in an e-mail, that e-mail may be disclosable to the individual concerned under the Data Protection Act.

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

6. Internet
6.1 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 using the IET-BYOD Wi-Fi 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.

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

6.3 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.

6.4 The IET employs web address filtering 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 3.1 of this policy.

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

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

7.3 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.

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

7.5 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.

7.6 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.
8. **PCs, Laptops & Printers**

8.1 The IT Service Centre will provide a standard desktop or laptop with the software required, for you to undertake your work, preinstalled. 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 ask the IT Service Centre.

8.2 The IT department will maintain appropriate backups of systems and servers including L and H drives - disk drives on desktops and laptops are not backed up.

8.3 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.

8.4 IET workstations are provided for business purposes.

8.5 No software or hardware should be installed without the authorisation of the IT Department who will ensure that appropriate steps are taken to ensure that the relevant licences are held and checks made before software or hardware is installed.

8.6 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.

8.7 Workstations and other IT equipment may not be transferred between users without reference to the IT Service Centre.

8.8 The IT Service Centre will provide all workstations with access/login controls and virus protection. Under no circumstances may users interfere with the normal operation of these facilities.

8.9 No attempt should be made to by-pass or disable any security arrangements installed or provided by the IT Department.

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

8.11 Workstations must be locked whenever you leave your desk to help protect against unauthorised access.

8.12 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.

8.13 Please remember that the security that applies to electronic information also applies when it is printed out. Do not print documents unnecessarily and ensure that printed documents containing sensitive information are shredded after they have been used.

8.14 The provision of printers within the IET is for business related printing and should not be used for personal printing unless there are exceptional circumstances.

9. **Portable storage**

9.1 Portable storage devices are such things as USB memory sticks but also include smart phones and other devices that have other primary functions but are capable of acting as storage devices when connected to computers.
Managers must consider the additional risk of loss or theft posed by portable storage devices when approving their use to hold sensitive or personal data.

Only encrypted USB drives which have been supplied by the IT Service Centre, should be used for personal or sensitive data.

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

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

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.

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

Cloud Storage

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

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

If you have a business requirement to use an alternative cloud storage service this should be discussed and agreed with your line manager, Information Security Officer and the Data Protection Officer.

Mobile Devices

Mobile devices (phones, iPads) 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.

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.

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.

Use of mobile devices in vehicles is subject to the policy on Driving on Company Business policy.

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.

An iPad “pool” is available for temporary loan purposes. Requests should be made to the IT Service Centre.
11.8 Diligent is the standard mobile app for use at board and committee meetings and must therefore be requested and justified as a separate item.

11.9 In cases of loss, theft, or unauthorised access please contact the IT Service Centre so that they can remotely disable and/or wipe the mobile device.

12. **Purchasing and Licensing**

12.1 All software and hardware must be purchased through the IT department. Requests for software and hardware should be made through the IT Service Centre.

12.2 The IET reserves the right to review all software installed on its PCs, to ensure that it is licensed and for business purposes. Any IET computer is subject to inspection (and any subsequent action) at any time by the employee’s line manager and the IT department to make sure that it is performing properly and is not running any unauthorised software.

12.3 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.

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

13. **IT Security Incidents**

13.1 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.

13.2 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.

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

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

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

13.4 As appropriate the IET’s Cyber Attack Response Plan will be followed.

14. **Related Policies and Procedures**

14.1 Disciplinary, Appeals and Suspension Policies
14.2 Disciplinary Regulations
14.3 Driving on Company Business policy
14.4 Display Screen Equipment Assessments
14.5 Information Security Policy
14.6 Data Classification Policy and Schedule
14.7 Password Guidance