ICT Users Policy

Corporate Owner:	ICT Manager
Contact Person:	Adrian Hudson
Applicability:	All Staff
Original Issue date	February 2018
Current Version Issue Date:	September 2018
Version:	1.04

Revision History

Revision Version	Date	Author	Description
1.0	26th February 2018	Michael Hynes	Draft Text
1.01	02nd May 2018	Michael Hynes	Amendments
1.02	18th May 2018	Ciaran Ward	Amendments
1.03	24th May 2018	Michael Hynes	Draft for Approval and Consultation
1.04	25th September 2018	Michael Hynes	Final

INDEX

1. Applicability and Objectives

This Policy is issued to provide guidance on proper usage of corporate IT resources. The Objective of the Policy is to ensure proper usage of corporate IT and telecommunication resources by the employees of Guildford Borough Council.

1.1 Introduction and General Provisions

Guildford Borough Council relies on its corporate network and IT systems to conduct its business. To ensure that its corporate network and personal computer (PC) resources are used properly by its employees and contractors, Guildford Borough Council's ICT Services has instituted this Corporate IT Policy.

It is the policy of Guildford Borough Council to maintain adequate standards of internal governance and a sound system of internal control processes and procedures. This document sets out the control standards and procedures that should exist in relation to this area. It is the responsibility of all service areas, to achieve the application and objectives of the policy. Should any exemption to this policy be required this needs the approval of the ICT Manager.

The term IT Systems refers to Guildford Borough Council's entire corporate network resources. Specifically, IT Systems includes, but is not limited to, personal computers and laptops, file servers, application servers, email exchange servers, fax servers, web servers, devices and communication facilities, corporate local and wide area networks and devices, Internet and extranets access, cloud based systems, voice systems (phones, voice recorders), printers, scanners, corporate business applications and other software installed on the personal computers and laptops.

The rules and obligations described in this Policy apply to all users of Guildford Borough Council (the users) corporate network, wherever they might be located. These rules also apply to any type of remote connection to the Guildford Borough Council corporate network. Violations will be taken seriously and could result in disciplinary action, including possible termination of employment, and civil and criminal liability.

1.2 Staff Responsibilities

Guildford Borough Council IT Systems are the property of Guildford Borough Council and may be used for business purposes only. It is every employee's duty to use Guildford Borough Council computer resources responsibly, professionally, ethically, and lawfully.

All staff are responsible for:

- complying with the policies set out in this document and with any specific instructions relating to IT Systems security as specified from time to time by senior management;
- ensuring the confidentiality of all business sensitive and personal data that they have access to;
- ensuring the physical security of all the IT equipment and magnetic media which is located and/or used in their Service;
- ensuring the security of portable IT equipment and magnetic media which they use off the premises in accordance with the procedures defined in this document;
- reporting any suspected security incident or security weakness to their Service Leader, in accordance with the procedures defined in this document;
- reporting any apparent software malfunction to their Service Leader, in accordance with the procedures defined in this document.

1.3 No expectation of privacy

The IT equipment and system accounts given to users are to assist them in the performance of their jobs. Users should not expect anything they create, store, send, or receive on the computer system to be private.

Users expressly waive any right to privacy when creating, storing, sending, or receiving anything on the computer or through the Internet or any other computer network. Users consent to allowing Management to access and review all materials users create, store, send, or receive on the computer or through the email, Internet or any other computer network. Users understand that Guildford Borough Council may use human or automated means to monitor use of its IT systems.

1.4 No expectation of ownership

All type of files, all types of electronic records, all types of software codes or related documents, and all types of data stored, created, implemented, or used on the Guildford Borough Council IT systems belong and are registered to Guildford Borough Council as the Data Controller or Processor. Users expressly waive any ownership rights.

1.5 Prohibited Activities

The following activities are strictly prohibited, and violation of any of them might lead to disciplinary actions and possible termination of employment.

Users must not:

- Send material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating; defamatory, or otherwise unlawful or inappropriate by email or any other form of electronic communication except where in the performance of their duties such as Safeguarding where such material forms part of the case file.
- Monopolize resources to the exclusion of others. That includes, but is not limited to, sending mass mailings or chain letters, extensive use of the business systems (aside from existing practice), spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network and systems traffic.
- Copy software or data files for use on their home computers;
- Provide copies of software or data files to any independent contractors or clients of Guildford Borough Council or to any third person without a Contract or Data Sharing Agreement;
- Install software or additional hardware on any of Guildford Borough Council workstations;
- Download any software from the Internet or other online service to any Guildford Borough Council workstations or servers (except those data files necessary for business);
- Modify, revise, transform, recast, or adapt any software;
- Disassemble computers, computer's accessories and other hardware or software, or de-compile any software. Users who become aware of any misuse of software or violation of the copyright law should immediately report the incident to their Service Leader;
- Physically relocate exchange or remove any ICT Systems equipment. Staff working from home may use their personal issue ICT equipment such as Laptops without restrict for business purposes. Personal issue equipment is not subject to the foregoing restriction.
- Install, play or transmit games or other entertainment software and files via ICT Systems facilities (email distribution, files sharing);
- Internet browsing and chatting for non-business purposes during business hours (see details elsewhere in this document);

- Spend an excessive amount of time on non-business phone calls;

Any exceptions to the above require prior written authorisation from the user's Service Leader and the ICT Manager.

2. Compliance with Legal and Contractual Requirements

2.1. Software Copying

Copyright material must not be copied without the owner's consent.

Computer software is normally supplied and used under the terms of a licence, which may specifically limit the use of that software to specific machines or a specific number of users. The licence normally also limits copying of the software.

Under no circumstances should software be copied either for use on the Council's premises or elsewhere without first referring to ICT Manager and obtaining their authority.

The ICT Service is responsible for ensuring that software is used and copied only within the terms of the relevant licence. A register of software will be maintained by the ICT Service and software usage audited on a regular basis.

2.2. Compliance with Data Protection and Secrecy Legislation

All staff must comply with the terms of local data protection and secrecy legislation.

It is the responsibility of the "Data Controller" * of any system to inform the local Data Protection Officer about any proposals to keep personal information on a computer. The Data Protection Officer is responsible for maintaining the Council's registration under Data Protection legislation and for advising Senior Management of legal requirements in this area.

3. Security

3.1. Security Incidents and Exception Conditions

Exception conditions (e.g. hardware failure, operational error, software fault) and security incidents must be reported promptly to the Line Manager to minimise the potential impact of such incidents.

Staff must report any exception condition, suspected security incident or security weakness of Guildford Borough Council computer systems or any other computer systems that contain the Council's data.

This includes:

- Suspected password compromise.
- Lost or stolen remote access token (such as SafeNet).
- Lost or stolen laptop, smart phone or other mobile computing device. This includes any personal mobile computing devices that may contain Council data.
- Lost or stolen removable storage media (CD-ROM discs, flash-drives and others). This includes any personal devices that may contain Council data.

Such incidents should be reported to ICT Services and their Manager as soon as possible to minimise damage. All issues will be escalated to IT management as appropriate.

Service Leaders must investigate any incident reported to them by their staff and report their findings to their Line Manager or ICT Management as appropriate.

3.2. Passwords

Individual computer users must use their unique login name and password to access the* Guildford Borough Council *IT systems and are responsible for maintaining the confidentiality of all passwords used in association with their IT systems.

Users are responsible for all transactions made using their passwords therefore no user may access any computer system with another user's account and password; including remote access token (SafeNet).

Passwords may be used for a number of purposes such as:

- Power-on passwords (used when switching on a PC).
- Network access passwords (to gain access to networked systems).
- Application passwords (to gain access to specific programs).
- File level passwords (used to protect individual files within applications such as Excel or Word).

All users must comply with the policies set out in The IT Password Policy document.

3.3. Hardware

All computer equipment and magnetic media must be properly secured.

All staff are responsible for ensuring the physical security of all the computer equipment and magnetic media which is located and/or used in their Service and for ensuring the security of portable computer equipment and magnetic media that they use off the premises.

3.4. Portable Computer Equipment

Individuals using portable computer equipment off the Council's premises are responsible for the security of both the hardware and any software and data files held on the equipment.

The following guidelines should be applied by users of portable computer equipment.

- When travelling, equipment and media must not be left unattended in public places.
- Portable computers should be carried as hand luggage when travelling.
- Portable equipment should not be left at home for longer than is necessary to complete a specific piece of work.
- Equipment should be marked with the Council's name and postcode.
- Equipment should be used for Council business only.

3.5. Access to Data

3.5.1. Unattended Equipment

Users should ensure that they do not leave terminals or PCs unattended whilst logged on to any business sensitive system.

Users must log off from any password protected application whenever they have finished using it and they must log out from the network at the end of each day.

Users may "lock" a PC workstation, which will be temporarily unattended if using non-password protected applications (e.g. MS Word). To lock the workstation, press the Ctrl+Alt+Del keys, the client options are displayed, select Lock. Unlock the workstation by entering your network password.

3.5.2. USB Pens and "Flash-drives"

Users must only use USB Pens and Flash-drives issued by ICT Services.

Users must take particular care of data stored on USB devices, flash-drives or similar devices. Only USB Pens and other similar devices issued by ICT Services must be used. These will require the use of a password to encrypt and secure the data stored on the device. All USB flash drives must be checked for Viruses and approved by the ICT Service before connecting to Council equipment.

3.5.3. Confidentiality of Business Data

Users must ensure the confidentiality of all business sensitive data that they have access to.

All staff are reminded that they have signed a contract undertaking and must not disclose any information regarding the affairs of the Council unless authorised to do so.

Users should control access to data on their PCs and terminals by following the procedures regarding passwords and unattended equipment set out above.

Computer output (whether by monitor display or printout) should not be accessible to other than genuine users.

When not in use, USB pens and other magnetic media should be kept in a suitable storage container and locked away at night.

Users may not alter or copy information belonging to another user without first obtaining permission in writing from the owner of the file or owner's Service Leader

A user's ability to connect to other computer systems through the network or by a remote access does not imply the right to connect to those systems or to make use of those systems unless specifically authorised by the ICT Manager and respective Service Leader.

Each user is responsible for ensuring that use of outside computers and networks, such as the Internet, does not compromise the security of Guildford Borough Council IT Systems. This includes taking reasonable precautions to prevent intruders from accessing the Council's network without authorisation and to prevent introduction and spread of viruses.

3.5.4. Encryption Software and Additional Security Passwords

Users may not install or use encryption software or install additional passwords on any of the Council's computers, files, and emails without first obtaining written permission from the ICT Manager and relevant Service Leader.

3.5.5. Data Protection and Secrecy Legislation

All staff must comply with the terms of data protection legislation.

Legislative requirements will differ from country to country and staff must ensure they abide by all local legislation. The six GDPR data protection principles set out below, which relate to personal data, are recommended as a guideline, these state that data shall be:

- Personal data must be processed lawfully, fairly and in a manner which is transparent to the data subject.
- Collection of personal data should be for specified and legitimate purposes;
- Collection of personal data should be adequate, relevant and limited to what is necessary;
- Accurate and where necessary kept up to date;
- Must be kept in a form which permits identification of data subjects for no longer than necessary and;
- Must be processed in a manner that ensures appropriate security of the personal data

Note: It is a legal requirement to register the use of personal data, therefore, advice should be sought from the Data Protection Team before any system (including spreadsheets and databases) which may contain personal data is developed.

3.6. Secure Disposal of Equipment and Storage Media

Data must be securely erased from all equipment and magnetic media prior to disposal.

Computer equipment must be disposed of in accordance with the Council's procedures for disposing of Fixed Assets. Additionally, any data held on such equipment or on associated magnetic media (disks, tapes, cartridges etc.) must be securely destroyed prior to disposal.

It is not considered adequate simply to delete data file directory entries as the underlying data can still be reconstructed.

Staff should advise ICT Services to arrange for the disposal of any storage media or computers.

4. System Management

4.1. Purchasing Equipment

4.1.1. Hardware and Software

Computer hardware and software may only be purchased with proper authorisation and through the approved channels.

Computer equipment and software must only be purchased through ICT Services, who will also advise on configuration, suitability, and costs before authorisation for expenditure is requested. All ICT purchases must be approved in advance by ICT Services.

4.1.2. Supplies

Supplies for use with computer equipment must be purchased through the approved channels.

Consumable supplies such as stationery, laser printer cartridges, printer, cleaning materials, stands, screen filters and paper should be obtained through Office Services.

4.2. Fault Reporting

4.2.1. Hardware Faults

All hardware faults must be advised to ICT Services.

ICT Services will determine (to the best of their ability) the nature of the problem and arrange for any hardware faults to be corrected by properly qualified maintenance engineers.

4.2.2. Operational Errors and Software Faults

Exception conditions (e.g. hardware failure, operational error, software fault) must be reported promptly to the appropriate member of management to minimise the potential impact of such incidents.

Software faults (or suspected faults) or Operational Errors must be reported to the ICT Service Desk at the earliest opportunity.

4.3. Computer Viruses

Virus detection and prevention measures must be applied at all times to minimise the risk of damage and loss of data.

Computer viruses and other malicious software often use weaknesses of email clients and office programs to infect other computers and/or steal information. An important component of protection for Guildford Borough Council computers is antivirus software. Antivirus software can identify and block many viruses before they can infect your computer. Particular care should be taken in respect of computer files attached to unsolicited external email and files downloaded from external sources such as the Internet.

Users must NOT-

- try to disable or uninstall your antivirus;

- bring in any software or data created or amended on PCs outside the Council. If the use of such software or data is required, then the disk (or other media) should be passed to ICT Services for checking before being used on any of the Council's PCs;

Users should

- be aware of unsolicited attachments, especially from people you do not know (this covers not only executable files, but also other files like images and office documents);
- if possible, check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments;
- not follow web links in unsolicited email messages;
- only use software and disks introduced through the approved channels on the Council's PCs;

4.4. System Housekeeping and Media Handling

4.4.1. Data and Software Back-up

Back-up copies of essential business data and software must be made on a regular basis and copies stored off-site.

In the majority of cases, where a Local Area Network is used, ICT Services will ensure that all volatile data stored on the network is backed up daily. Users are advised that PC data must be stored on the LAN (i.e. NOT the C: drive or D: drive)

Where the PC is operating in a "stand alone" situation or where data must be held on the local hard disk for some other reason, then it is the user's responsibility to ensure that adequate backup copies are taken. Advice should be sought from ICT Services to ensure an appropriate backup strategy is used. Users must not take backup copies of data home for storage. Where it is important to store backup copies of data off-site, then appropriate arrangements must be made with ICT Services.

4.4.2. Housekeeping and File Management

Users are responsible for all "housekeeping" and file management relating to PC files.

Users must perform regular housekeeping of both their local hard disks (normally "C:" drive); network drives and e-mail systems and delete any files that are no longer required. Users should organise their files into logical directories to make file management easier and to speed up file retrieval. Where necessary, assistance should be sought from ICT Services.

5. Applications

5.1. Authorisation to Use Applications

All authorisations to use the IT Systems and IT Services are regulated through the IT Request form (available on the Loop under ICT Services)

The IT Request form normally covers:

- New user installation (that requires an approval collection from the HR Service);
- Corporate application installation (those specified in the ICT Request);
- Additional access within IT Systems (including access to other (or resigned) users home drives or emails);
- PC upgrades (including memory only upgrade);
- User account amendments (including user name change);
- Any equipment relocations (including PCs, phones, other workstations).

All the exceptions to the IT Request Forms to be separately authorised by the Service Leader and ICT Manager.

5.2. Spreadsheets and Databases

It is particularly important that critical data held in spreadsheets or databases is verified against its source and wherever possible the data should contain an appropriate identifier which allows an audit trail to be maintained.

- Complex and critical spreadsheets and databases should be carefully tested before output is relied upon.
- Appropriate documentation must be maintained (preferably within the spreadsheet itself) which fully explains how the spreadsheet or database works.
- The Council's Spreadsheet Standards must be applied to all Business Critical spreadsheets.
- Where necessary, assistance should be sought from ICT Services.
- Particular care should be taken when sending a spreadsheet to a member of the public in response to a Freedom of Information request. Spreadsheets should be checked thoroughly for any hidden data which may be confidential or sensitive and could therefore result in a data breach if inadvertently released into the public domain.

6. Internet and Email

The sub-sections below highlight the main policy issues that all users should be aware of. The Council's policy relating to Internet and email is set out in detail in the Information Systems Policy document and must be followed by all users.

Any employee that misuses the Council's email, internet or other communication facilities will be subject to immediate disciplinary actions.

6.1. Personal Use of the Council's Internet and E-mail Services

Limited use of the Council's Internet and E-mail services may be made for personal reasons; however, such use is strictly restricted and must not interfere with Council business.

6.2. Internet Services

Internet access, particularly web browsing, is provided for authorised business use. All web sites that are browsed may be recorded by the Council's Internet system and are subject to management review at regular intervals.

All Staff using these services must adhere to the policies defined in the Information Systems Policy manual which will be available on the intranet. In particular, it should be noted that:

6.2.1. Internet Browsing and Downloading of Data

Guildford Borough Council ***is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network; users are cautioned that many of Internet pages include offensive, sexually explicit and inappropriate material. Users accessing the Internet do so at their own risk.***

All Staff using these services must adhere to the following policies:

- Access to the Internet during normal working hours is for business use only.
- Staff must not access, display, store or distribute any web page which, on the widest interpretation, could be regarded as illegal, unlawful, offensive, in bad taste or immoral. This definition is to be interpreted very widely: content may be perfectly legal in the UK, yet in sufficient bad taste to fall within this prohibition. As a general rule, if any person within the Council (whether they intended to view the page or not) might be offended by the contents of a page, or if the fact that the Council's software had accessed the page might embarrass the Council if made public, then it may not be viewed.
- The same rule applies to any files or data (whether documents, images or other) obtained from the Internet.
- Under no circumstances should software or any executable program files be copied or downloaded or installed whether from the Internet or otherwise, either for use on the Council's premises or elsewhere without first making reference to ICT Services or obtaining their authority.
- Any software or files downloaded from the Internet become the property of the Council.
- Internet facilities may be used for personal reasons during an employee's lunch break or outside working hours provided that all usage policies are adhered to and in the Council's opinion does not interfere with the Council's business.
- Employees must not use the Council's Internet facilities to download entertainment software or games, or to play games over the Internet.

- Usage of the ICQ, MSN, Skype or similar facilities is prohibited unless is it is authorised by the relevant Service Leader (through the IT Request form).

6.2.2. Monitoring of Internet Use

Internet use will be monitored to ensure compliance with these policies.

6.2.3. Publishing Data on Internet (inc. Newsgroups and Chat-rooms)

Staff who are not authorised, must not speak about the Council or its business on any Internet based forum.

6.3. E-mail Services

Internal and external e-mail services are provided for authorised business use.

E-mail services are provided to allow staff to communicate efficiently and effectively with colleagues, customers and other parties as required in the normal course of business.

All Staff using these services must adhere to the policies defined in the Information Systems Policy manual. In particular, it should be noted that:

- The use of the Council's email systems to transmit unacceptable or offensive material may lead to disciplinary action.
- The transfer of confidential information of the Council over the Internet (Guildford Borough Council) is prohibited, unless separately authorised by the Service Leader or Director.

6.3.1. Appropriate Use of E-mail

For legal purposes, an e-mail is treated by a Court as being no different to any other written communication. Therefore, you should not put into an e-mail message anything that you would normally be unprepared to put into a memorandum, letter or other written form of communication.

Your messages represent the Council - hence all outgoing messages must be written in the highest ethical and professional standard.

Every employee should use an electronic signature in the following format

First name Last name
Position (Optional)
Guildford Borough Council
Tel.
Mobile (optional)
e-mail

6.3.2. Content of E-mails (internal or external)

All staff must take particular care about what they say in e-mail messages, whether in internal e-mails only or in external e-mails to customers or any other persons or organisations. Improper statements may give rise to personal liability for the member of staff concerned and/or liability for the Council. Staff should also be aware that anything they say in an email about an individual (whether an employee or third party) could be requested by the individual concerned via a Subject Access Request (SAR).

6.3.3. Confidentiality

Staff must not send confidential information concerning the Council, its business or its customers to any third party without appropriate internal authorisation to do so. If authorisation is approved, such any emails must be sent securely and marked "PROTECT" or "RESTRICTED", depending on the level of confidentiality of the information being sent.

6.3.4. Data Protection

Staff must not include personal data in e-mail messages without first obtaining consent from the individual concerned.

6.3.5. Internet Based E-mail Accounts

The use of Internet based e-mail accounts, such as Microsoft "Hot-Mail", is not permitted for business use.

6.3.6. Monitoring of E-mail for Computer Viruses

The Council will use automated "content monitoring" systems to enforce the above restrictions. In particular systems will be used to detect computer viruses, obscene or inappropriate language and inappropriate images in e-mail messages.

6.3.7. Monitoring of E-mail Use

The Council expressly reserves the right to monitor the use at work of Internet and e-mail, at its discretion, if it considers that there may have been or may be a breach of these policies.

6.3.8. Retention of E-mails

For record keeping purposes, Staff should treat e-mails as they would any other written communication such as a letter, report or memorandum. Therefore, hard copies of e-mails that are necessary for record keeping purposes must be printed and kept in an appropriate paper file.

6.3.9. E-mail Service Standards

Mailbox Size
Standard mailbox size is 1000 Mb (exceptions must be authorised by Service Leader and ICT Manager); users are responsible for cleaning up excessive size of the mailbox by deleting/archiving unnecessary messages.

When a user approaches their mailbox limit (1000Mb) an informational email may be generated, requiring them to perform mailbox clean-up.

Virus and Spam protection
All incoming emails are automatically checked for viruses

Junk email folder
Guildford Borough Council ICT systems are protected from external spam messages by an anti-spam system that inspects all incoming messages and filter them out based on the suspicion of the spam. **All suspected messages are automatically quarantined and a message sent to the recipient (and are not delivered to the Inbox)**.

Users are responsible for reviewing the Junk Email folder in case of any business correspondence is moved to this folder.

7. Telephony Policy

7.1. Personal Use of Telephone Systems

Telephones, mobile phones, Samsung and other similar devices are provided primarily for business use, however it is accepted that staff may occasionally need to use a telephone or mobile phone for personal reasons.

- Personal calls must be kept to an absolute minimum.
- Personal calls to overseas numbers may only be made with the permission of the Service Leader.
- Particular care must be taken when using mobile phones overseas as call costs can be expensive – these must therefore be kept to the absolute minimum time.
- Calls must not be made to premium rate numbers.
- The Council's policies relating to email and Internet use apply also to Smartphones and similar devices (see relevant sections of this manual for full details)
- Telephones are available that are not recorded. These may be used if a member of staff works in an area where telephone lines are normally recorded and they wish to make an unrecorded private phone call in line with the above policy.
- Staff will be asked to recompense the Council for personal calls above a minimal amount (such amount to be advised separately from time to time).

7.2. Office Telephones

Access to international calls is available to authorised users on their own phones (if service is unavailable an authorisation can be obtained via Service Leader).

Making international calls from another employee's phone is strictly prohibited.

7.3. Mobile Phones / Smartphones

Guildford Borough Council provides corporate mobile phones and / or Smartphones for authorised employees. Your corporate mobile number will be added to Corporate Address Book and will be available for all employees.

All mobile devices connected to Guildford Borough Council network must have PIN protection enabled. Loss or theft of any mobile device containing corporate data must be reported to ICT Service Desk immediately.

Further information relating to Mobile Phones is published in the Mobile Phone Policy document.

8. Health and Safety Policy

Any concerns regarding Health and Safety should be referred to your Line Manager.

8.1.1. Location and Installation of Computer Equipment

Computer equipment must be installed with due consideration to Health and Safety requirements.

When computer equipment is installed, the location and positioning of the equipment must take account of the comfort, health and safety of the user(s). In particular, Health and Safety regulations must be complied with. As a minimum, consideration should be given to the following matters:

- Staff should never move fixed computer equipment without assistance from either ICT Services or Office Services.
- The screen should be placed at a comfortable height (adjustable stands should be provided if required).
- Glare from windows or lights should be avoided if practically possible, if not then appropriate anti-glare screen filters should be used.
- The keyboard should be placed at a comfortable height, distance and angle for the user.

All cables and wires should be stowed safely (in particular they should NOT trail across the floor).