27. ICT Acceptable Use Policy

27.1 Policy statement

This policy sets out the Council's requirements for ICT Acceptable Use.

27.2 Purpose

Council staff, contractors and Councillors will be required to have access to the Council's ICT systems, applications and equipment in the performance of their duties in order for them to carry out their business. For all users of the Council's ICT facilities, this policy describes the Council's position on acceptable usage.

27.3 Scope

This policy applies to all users of the Council's ICT facilities whether this is at work, at home or elsewhere. The policy applies to all users who may be employees, contract staff, temporary staff, volunteers or Councillors.

27.4 Risks

Oxford City Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- The non-reporting of information security incidents,
- Inadequate destruction of data,
- The loss of direct control of user access to information systems and facilities etc.
- Misuse of the Council's ICT facilities

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers.

27.5 User responsibilities

Users of ICT facilities are responsible for:

- Informing their manager (or in the case of councillors the Head of Law and Governance) if they believe that others are using systems inappropriately.
- Notifying the ICT Service Desk if they believe that their personal login details have become known to another person.
- Safeguarding personal data.
- Contacting the ICT Service Desk if they suspect a virus infection.
- Ensuring that personal use of Oxford City Council ICT equipment remains occasional and reasonable and does not interfere with everyday workload and commitments or endanger the Council's ICT services.

27.6 Managers responsibilities

Managers are responsible for ensuring that all their employees are aware of this policy and act in accordance with its requirements (or in the case of councillors the Head of Law and Governance).

27.7 Privacy

All systems may be monitored and audited for administrative and management purposes so personal privacy cannot be assumed.

Systems may be accessed in exceptional circumstance at management discretion during an individual's absence to ensure continuation of business.

27.8 Policy compliance

If any member of staff is found to have breached this policy, they may be subject to Oxford City Council's disciplinary procedure. Any breaches of the policy by elected members would be treated as code of conduct complaints. Members can seek further advice from Committee and Member Services.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager (or in the case of councillors the Head of Law and Governance).

27.9 Infrastructure security

- Desktop PCs should not have data permanently stored on the local hard drive.
- Network drives must be used to store data and documents.
- A laptop hard drive may be used only temporarily to retain documents being moved from one system to another.
- Use of Council equipment by friends or family is strictly forbidden.
- Staff should be aware of their responsibilities in regard to the Data Protection Act.
- Equipment that is to be reused or disposed of must have all of its data and software erased / destroyed.

27.10 Removable media

- All data stored on removable media devices must be encrypted where possible.
- Damaged or faulty removable media devices must not be used.
- Care must be taken to physically protect the removable media device and stored data from loss, theft or damage.
- Removable media devices that are no longer required, or have become damaged, must be returned to ICT Services for secure disposal.
- Removable media devices should be used only for the transfer of data and not for permanent storage.

27.11 ICT access

- Passwords must be protected at all times and must be changed when prompted.
- It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems.

- Partner agencies or third party suppliers must contact the ICT Service Desk to enable any connection to the Oxford City Council network.
- Staff shall not permit third party access without prior consent from the ICT Service Desk.

27.12 Remote access

- It is the user's responsibility to use portable computer devices in an acceptable way. This includes not installing software, taking due care and attention when moving portable computer devices and not emailing "OFFICIAL and above information" to a non-Council email address.
- Users should be aware of the physical security dangers and risks associated with working within any remote office or mobile working location.
- It is the user's responsibility to ensure that access to all "OFFICIAL and above information" is controlled.
- All "OFFICIAL and above data" held on portable computer devices must be encrypted.

27.13 Software policy

- All software acquired must be purchased through ICT Services, subject to scrutiny.
- Under no circumstances should personal or unsolicited software be loaded onto a Council machine.
- Every piece of software is required to have a licence and the Council will not condone the use of any software that does not have a licence.
- Changes to software must not be made by users or third parties, without prior consent from the ICT Service Desk.
- Users are not permitted to bring software from home (or any other external source) and load it onto Council computers.
- Illegal reproduction of software is subject to civil damages and criminal penalties.

27.14 Email

- All emails that are used to conduct or support official Oxford City Council business must be sent using the "@oxford. gov.uk" email address.
- All emails sent via the Government Connect Secure Extranet (GCSx) must be of the format "@oxford.gcsx.gov.uk".
- Non-work email accounts must not be used to conduct or support official Oxford City Council business.

- Councillors and users must ensure that any emails containing sensitive information must be sent from an official Council email.
- All “OFFICIAL and above” external e-mail must carry the official Council disclaimer.
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the Council’s Equal Opportunities Policy.
- Where GCSx email is available to connect the sender and receiver of the email message, this must be used for all external email use and must be used for communicating “OFFICIAL and above” material.
- In no circumstances is automatic forwarding of email permitted. Auto-forwarding affords no control or protection against the accidental forwarding of personal, private, or sensitive information out of the Council, and as a consequence, leaves the Council open to the risk of potential data breaches and fines.

27.15 Internet use

- Provided it does not interfere with your work, the Council permits personal use of the internet in your own time (for example during your lunch break).
- Users must not create, download, upload, display or access knowingly, sites that contain pornography or other “unsuitable” material that might be deemed illegal, obscene or offensive.
- The laws concerning the protection of copyright and intellectual property rights must be respected.
- Downloading and storage of music and video files and images without a bona fide business reason is forbidden.
- Users must assess any risks associated with internet usage and ensure that the internet is the most appropriate mechanism to use.
- Users must not subscribe to, enter, or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Users must not enter or use online gaming or betting sites.
- Users must not subscribe to or enter “money making” sites or enter or use “money making” programs.
- Users must not run a private business via the internet from Council equipment or premises.
- On-line shopping from a secure site is permitted in the user’s own time but the Council has no liability for any transaction and goods should not normally be delivered to the workplace.

The above list gives examples of some “unsuitable” usage but is neither exclusive nor exhaustive. “Unsuitable” material would include data, images, audio files or

video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other Council policies.

27.16 Use of fixed line phone, mobile phones and smart phones

- Users should ensure that, as far as practicable, private phone calls are restricted to non-work time.
- Users must comply with the Council's specific prohibition on the use of mobile phones when driving on Council business.
- Mobile phones should not be used to distribute, receive or store any material which is offensive or prohibited.

27.17 Government Connect & Information Protection

Information Protective Marking (IPM) is an information security classification scheme that requires the prominent marking of information and documents with a short standard wording that indicates how the information should be handled from a security point of view.

A document should be protectively marked either if there would be significant impact to the Council if the confidentiality, integrity or availability of the document was compromised. If you are the 'originator' of a document or record (i.e. the author or someone responsible for receiving and / or distribution) then you are responsible for adding a protective marking if it is not already marked.

- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the HMG Security Policy Framework (SPF). (Appendix 1).
- Information sent via the Government Connect Secure Extranet (GCSx) must be labelled appropriately using the SPF guidance. (Appendix 1).
- Access to information assets, systems and services must be conditional on acceptance of the Acceptable Use Policy.
- OFFICIAL information must not be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Disclosing OFFICIAL classified information to any external organisation is also prohibited, unless via the GCSx email.
- Where GCSx email is available to connect the sender and receiver of the email message, this must be used for all external email use and must be used for communicating OFFICIAL material.
- The disclosure of OFFICIAL classified information in any way other than via GCSx email is a disciplinary offence.

Appendix 1 – HMG Security Policy Framework

All information assets must be classified and labelled in accordance with the HMG Security Policy Framework (SPF). The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification.

The SPF requires information assets to be protectively marked into one of 3 classifications. HMG operates a Classification Policy to identify and value information according to its sensitivity and to drive the right protections. This comprises three levels: OFFICIAL, SECRET and TOP SECRET for which there are distinct security arrangements. OFFICIAL covers most of the day-to-day business of government, service delivery, commercial activity and policy development.

Further details can be found here:
https://www.gov.uk/government/publications/security-policy-framework

Appendix 2 – Exclusions

This policy excludes non-electronic forms of data and information which shall be subject to non-ICT policies within the Council.

This page is intentionally left blank