ICT Services
ICT Acceptable Use Policy

Contents

ICT Services
ICT Acceptable Use Policy

1. Policy Statement

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

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.

3. Scope

This policy applies to all users of the County 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

4. Risks

Oxfordshire County 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 Councils 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**.**

5. User Responsibilities

As a user of ICT facilities, you are responsible for:

- Informing your manager under the Raising Concerns at Work procedure if you believe that others are using systems appropriately
- Notifying the ICT Service Desk if you believe that your personal login details have become know to another person
- Safeguarding personal data
- Contacting the ICT Service Desk if you suspect a virus infection
- Ensuring that personal use of Oxfordshire County Council ICT equipment remains occasional and reasonable and does not interfere with everyday workload and commitments or endangers the Council's ICT services
- Understanding this policy and completing the on-line ICT Acceptable Use course provided by Oxfordshire County Council

ICT Services
ICT Acceptable Use Policy

6. Managers Responsibilities

Managers are responsible for ensuring that all their employees are aware of this policy and act in accordance with its requirements

7. Privacy

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

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

8. Policy Compliance

If any user is found to have breached this policy, they may be subject to Oxfordshire County Council's disciplinary procedure. 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.

9. Policy Governance

The following table identifies who within Oxfordshire County Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Head of ICT Services
Accountable	Asst Chief Executive & Chief Finance Officer
Consulted	Asst Head of Finance (Audit), HR Business Partner, Head of Legal Services, Information Governance Group
Informed	All Council Employees and Contract staff, Councillors

ICT Services
ICT Acceptable Use Policy

10. Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by Deputy Head of ICT Services

11. References

The following County Council policy documents are directly or indirectly relevant to this policy:

- Email Policy
- Software Policy.
- ICT Access Policy.
- Removable Media Policy.
- Human Resources Information Security Standards.
- Information Security Incident Management Policy.
- Communications and Operation Management Policy.
- ICT Infrastructure Policy.
- Computer, Telephone and Desk Use Policy.
- Remote Working Policy.
- Legal Responsibilities Policy.
- Information Protection Policy.

All these policies may be found on the County Council's Intranet.

12. Infrastructure Security

- Desktop PCs should not have data stored on the local hard drive
- Document Manager and 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 OCC equipment by friends or family is strictly forbidden
- Non-electronic information must be assigned an owner and a classification. PROTECT or RESTRICTED information must have appropriate information security controls in place to protect it.
- 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.

ICT Services
ICT Acceptable Use Policy

13. Removable Media

- It is Oxfordshire County Council policy to prohibit the use of removable media devices. The use of removable media devices will only be approved if there is a valid business case for its use.
- Any removable media device that has not been supplied by ICT **must not** be used.
- 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

14. 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 3rd party suppliers must not be given details of how to access the Council's network
- Partners or 3rd party suppliers must contact the ICT Service Desk to enable any connection to the Oxfordshire County Council network

15. 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 PROTECT or RESTRICTED 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 PROTECT or RESTRICTED information is controlled
- All PROTECT or RESTRICTED data held on portable computer devices must be encrypted.

ICT Services
ICT Acceptable Use Policy

16. Software policy

- All software acquired must be purchased through ICT Services
- 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.
- 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.

17. Email

- All emails that are used to conduct or support official Oxfordshire County Council business must be sent using a "@Oxfordshire. gov.uk" address.
- All emails sent via the Government Connect Secure Extranet (GCSx) must be of the format "@oxfordshire.gcsx.gov.uk".
- Non-work email accounts must not be used to conduct or support official Oxfordshire County Council business
- Councillors and users must ensure that any emails containing sensitive information must be sent from an official council email.
- All official 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 PROTECT and RESTRICTED material.
- Automatic forwarding of email must be considered carefully to prevent PROTECT and RESTRICTED material being forwarded inappropriately.

18. 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 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.

ICT Services
ICT Acceptable Use Policy

- Users must not enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs.
- 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

19. Use of Phones/Mobile Phones/Blackberries

- 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
- When Council equipment is used for personal texts or calls, these must be paid for by the user

20. Government Connect & Information Protection

- All information assets, where appropriate, must be assessed and classified by the owner in accordance with the HMG Security Policy Framework (SPF). (See Appendix 1)
- Information up to RESTRICTED sent via the Government Connect Secure Extranet (GCSx) must be labelled appropriately using the SPF guidance.
- Access to information assets, systems and services must be conditional on acceptance of the Acceptable Use Policy.
- PROTECT and RESTRICTED information **must not** be disclosed to any other person or organisation via any insecure methods including paper based methods, fax and telephone.
- Disclosing PROTECT or RESTRICTED 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 PROTECT or RESTRICTED material.
- The disclosure of PROTECT or RESTRICTED classified information in any way other than via GCSx email is a disciplinary offence

ICT Services
ICT Acceptable Use Policy

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. Information up to RESTRICTED sent via GCSx must be labelled appropriately using the SPF guidance.

The SPF requires information assets to be protectively marked into one of 6 classifications. The way the document is handled, published, moved and stored will be dependant on this scheme.

The classes are:

- Unclassified.
- PROTECT.
- RESTRICTED.
- CONFIDENTIAL.
- SECRET.
- TOP SECRET.

ICT Services
ICT Acceptable Use Policy

Development of this policy was assisted through information provided by the following organisations:

- Devon County Council
- Dudley Metropolitan Borough Council
- Herefordshire County Council
- Plymouth City Council
- Sandwell Metropolitan Borough Council
- Sefton Metropolitan Borough Council
- Staffordshire Connects
- West Midlands Local Government Association
- Worcestershire County Council