

ICT Acceptable Use Policy



EAST RIDING
OF YORKSHIRE COUNCIL

Lead Directorate and Service:	Corporate Resources - Digital Change and Technology
Effective Date:	December 2022
Contact Officer/Number:	David Cox - ICT Security Manager
Approved By:	Cabinet

Contents

ICT Acceptable Use Policy	1
1. Introduction	1
2. Definitions for the Purposes of this Policy.....	1
3. Scope.....	1
4. Policy Statement.....	1
5. Corporate Requirements	1
6. Policy Development Including Consultation.....	2
7. Links with Other Policies.....	2
8. Policy Implementation	2
9. Policy Compliance.....	6
10. Financial Implications	6
11. Review	6

ICT Acceptable Use Policy

1. Introduction

East Riding of Yorkshire Council (ERYC) are making ever increasing use of Information and Communication Technology (ICT) and customer information held by the council and other public sector organisations. The information that ERYC holds, processes, maintains and shares with other public sector organisations is an important asset that, like other important business assets, needs to be suitably protected.

The EU General Data Protection Regulation 2016 (GDPR), the UK Data Protection Act 2018 (DPA 2018) and The Privacy and Electronic Communications (EC Directive) Regulations 2003 which in combination constitute 'the legislation', determines how individuals' personal information is processed and kept safe.

It is unlikely that any policy can cover all circumstances that may arise. This policy does not contain an exhaustive list but emphasises the standards of performance and behaviour which are expected of employees and defines what constitutes acceptable use. Common sense and sound judgement are required on the part of managers in the fair and consistent application of this policy for employees.

2. Definitions for the Purposes of this Policy

For the purpose of this Policy the key definitions are:

Computer User: Any member of staff using an East Riding of Yorkshire Council IT asset in pursuit of their duties associated with their post(s) for the council.

ICT Equipment/IT Assets: This policy applies to the use of all information

systems, devices and IT services owned or leased by ERYC

3. Scope

This Policy applies to all employees, councillors, committees, partners and contractual third parties and agents of ERYC who access and utilise council ICT owned facilities and equipment.

4. Policy Statement

This Policy documents how a user should use council ICT equipment/IT assets. It will outline the user's personal responsibilities and inform them of what they can and cannot do.

East Riding of Yorkshire Council will ensure that every user is aware of and understands the acceptable use of the council's computer resources.

5. Corporate Requirements

ICT Security is vital to the effective operation of ERYC. All ICT equipment used by the council must adhere to the highest standards of ICT security at all times so that:

- The public and all users of the council's information systems are confident of the confidentiality, integrity and, availability of the information used and produced.
- Business damage, interruption and reputation caused by security incidents are minimised.
- All legislative and regulatory requirements are met.
- The council's ICT equipment and facilities are used responsibly, securely and with integrity at all times.

6. Policy Development Including Consultation

This Policy has been developed in consultation with:

- Corporate Management Team.
- Senior Management Team.
- Information Governance Management Board.
- Portfolio Holder.
- Head of Digital, Change & Technology.
- Head of Legal and Democratic Services and Senior Information Risk Owner (SIRO).
- Head of Human Resources.
- Data Protection Team.
- ICT Management Team
- ICT Security Manager.

7. Links with Other Policies

The following East Riding of Yorkshire Council Policy documents are directly relevant to this Policy and are referenced within this document:

- Information Management Strategy
- ICT Strategy and Technical Framework
- ICT Security Policy.
- Policy and Guidelines on the use of electronic mail (email).
- Policy and Guidelines on the use of the Internet.
- Records Management Policy.
- Use of council Resources.
- Data Protection Policy.
- Cyber Incident Response Policy
- ICT BYOD Policy
- ICT Firewall Change Management Policy
- ICT Patch Management Policy
- Third Party ICT Access Policy
- Policy and Guidance for Web Application Penetration Testing

8. Policy Implementation

Key Messages

- Staff are responsible for the upkeep of the IT Asset Manager. All moves and disposals should be actioned via this process.
- IT equipment not detailed correctly on the IT Asset Manager will be refused access to the council's network and will not be supported.
- All IT equipment and software must be purchased through the council's supplies service.
- All passwords must be strong as detailed in the ICT Access section of the ICT Security Policy.
- All data stored on removable media devices must be encrypted.
- All users must be aware of their legal obligations.

Personal Use

IT equipment can be used for personal use by staff, so long as it is not used in relation to an external business or is not used in a way that could cause reputational damage to the council or its residents.

The following uses of ERYC's IT and Information Systems are not permitted under any circumstances:

- To pursue personal business, financial or political interests.
- Participation in any form of chain letter or the sending of unsolicited email (spam).
- Taking another person's identity by using their password without permission, forging messages, posting anonymous messages or gaining unauthorised access to internal/external computer systems (malicious activity or hacking).
- Any activity that corrupts or destroys other user's personal data.

- Activities that disrupt the work of others.
- To commit fraud (including bribery and/or corruption), theft, or for any other illegal purpose.

All work-related corporate communication, including telephone calls, text messages, emails and contributions to social media websites and internet-based applications must conform to the relevant guidance available on the council intranet.

When using ERYC information systems, it is strictly forbidden to deliberately or maliciously create, access, view, download, transfer, print and/or disseminate any material which is likely to be interpreted as extremist, offensive, harassment, discrimination, incitement to hatred/violence, pornographic or any other material that could bring the council into disrepute. Employees must immediately report any accidental access to such material to your line manager.

Asset Management

All users are responsible for keeping their assets up to date using the web-based IT Asset Manager. Any movements, reallocations or disposal of IT equipment must be updated by the end user or their line manager on the IT Asset Manager.

It is the responsibility of each section head to undertake an annual IT compliance check, ensuring that all assets are correctly assigned on the IT Asset Manager and that all IT equipment conforms to the council's approved refreshment programme.

Use of Software

The ability to buy and install software is restricted to ensure that there is a complete record of all software that has been purchased for ERYC ICT devices, that all software is legal, doesn't contain any viruses or other malware and can be supported and upgraded by IT Services

All software acquired by ERYC must be approved by and purchased through IT Services, utilising the Procurement Process

You may not use or permit the use of any software, other than software provided by the council. You must not attempt to change, alter or delete the software or the configuration of the software installed on your computer. IT Services will remove software that is unregistered or unlicensed.

Use of Hardware

All Technology provided to you is for council use. It remains the property of ERYC and you may be required to return it at any time. You must not allow it to be used by non-council employees or use it to carry out a third party's instructions, except in the proper performance of your role and in accordance with this policy.

You must report any actual or suspected loss, theft, breach, unauthorised access or damage to your Computer, council issued Smartphone, Portable Device, Removable Media or other Technology immediately to your line manager, IT Service Desk and the Information Governance Team within 24 hours

You must take reasonable care to protect any technology which is issued to you. If technology is lost or damaged while in your possession, inform your line manager and the IT Service Desk immediately. You may be required to account for the measures you took to reduce the risks of loss or damage.

You must not destroy or modify, or attempt to destroy or modify, any IT equipment unless you are expressly authorised to do so. Any IT equipment that is damaged or no longer required should be returned to IT Services to be securely disposed of. Do not use IT equipment that is damaged.

Saving Files and Documents

Files and documents must be secured appropriately for the classification applied. All council related business files and documents including electronic information must be stored on the council's secure network for on premise services, and any file or document containing personal information **MUST** be secured for limited employee access in the correct area to avoid a personal data breach occurring. If you are unsure as to what level of security a file or document has, you should check before saving the information to the network. Do not use your computer hard drive (C:).

Staff should ensure that good housekeeping procedures are followed. These include the use of an appropriate directory/folder structure on personal network drives and shared network drives and regular removal of unwanted files.

It is not permitted to store private documents or images on any council IT equipment.

Removable Media

All users must be aware that special attention must be paid when using any attached storage device

- Any removable media device used to conduct official council business must only be purchased and installed by IT Services. Any removable media device that has not been supplied by IT must not be used to store council data without prior permission from the ICT Service.
- All data stored on removable media devices must be encrypted.
- All personal and sensitive data or **OFFICIAL-SENSITIVE** data stored on removable media must always be

hardware encrypted current NCSC standards.

- Only data that is authorised and necessary to be transferred should be saved on to the removable media device.
- Removable media devices must not to be used for archiving or storing records as an alternative to other storage equipment.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage. Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage, loss or theft.

For advice or assistance on how to securely use removable media devices, please contact the IT Service Desk.

Passwords

All users must be aware that it is of utmost importance that their password remains protected at all times.

The following guidelines must be adhered to at all times:

- Never reveal your passwords to anyone.
- Never use the 'remember password' function.
- Never write your passwords down or store them where they are open to theft.
- Never store your passwords in a computer system without encryption.
- Do not use any substantial part of your username within the password.

- Do not use the same password for systems inside and outside of work.
- Do not email passwords.

Security Software

IT equipment must be connected to the corporate network at least once every 14 days to ensure that all antivirus software updates and patches are applied. For remote users this can be done by connecting to the council's network using the AnyConnect VPN solution.

Where a virus is detected on a council system the individual must immediately report it to the IT Service Desk.

Internet, Intranet, Social Media Websites and Electronic Publishing

Internet access is provided to enable you to access information and systems that are relevant to your role. You must not intentionally store or transmit copyrighted material without the permission of the owner. You must not access inappropriate unsuitable websites which include websites that contain or portray unsuitable material including, but not limited to:

- Pornography
- Extremist material
- Violence
- Hate or discrimination
- Hacking
- Gambling

Information available on the council Intranet is confidential and intended solely for use by council employees. You must not disseminate or distribute information from the council intranet site to anyone who is not, or who may not be, authorised to receive it.

If your role involves responsibility for publishing information on the intranet or internet, including social media websites, blogs and associated internet applications, you must:

- keep the material up to date
- ensure that material does not compromise the council's intellectual property
- ensure that material does not misrepresent the council or cause embarrassment to the council or its employees
- comply with the Data Protection Act 2018 when publishing material
- not publish personal opinions.

The Policy and Guidelines on the use of the Internet sets out how council staff should utilise the Internet.

Monitoring

The council's IT service may in certain circumstances monitor the use of:

- IT systems and associated technologies
- council supplied mobile phones and voice mail
- desk phones and voice mail
- the internet
- council email

The council may request a hardware or software audit of the technology issued to you, an audit may also require IT devices to be taken from you and you must comply with any such request

The council may also access a user's email account in the event of an unexpected or prolonged absence to ensure continuity of service.

Email

The Policy and Guidelines on the use of electronic mail sets out how the council email service is to be used

Connectivity

All physical devices connected to the council's network must be approved by the

ICT Service. Personal devices must never be connected to council equipment or the council network.

9. Policy Compliance

If any user is found to have breached this Policy, they may be subject to East Riding of Yorkshire 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 the IT Service Desk or ICT Service.

10. Financial Implications

The requirement to ensure appropriate protection of the council's corporate infrastructure is one that can be managed within existing budgets.

11. Review

This policy will be reviewed on an annual basis unless there is a major changes or security-event, then the policy will be resolved.

