ICT Acceptable Use Policy

1 Version History details and author

1.0	27/07/2011	Completed for distribution	Jo White
1.0	24/08/2011	Approved by Information Governance Group	Jo White
2.0	31/10/2012	Reviewed by Information Governance Group	Jo White
3.0	29/11/2013	Reviewed by Information Governance Group. Section 4.5 inserted re Personal Devices.	Jo White
4.0	12/01/2015	Reviewed by Information Governance Group. Remove use of email, geotagging on phones to be switched off, no recording on personal devices.	Jo White
5.0	11/05/2015	Reviewed by Information Governance Group. Reference to information handling added.	Jo White
6.0	03/09/2015	Reviewed by Information Governance Group. Reference to Hardcopies added.	Jo White
7.0	10/10/2016	Reviewed by Information Governance Group. Personal devices not to be plugged in to DCC equipment.	Jo White
8.0	06/11/2017	Reviewed by Information Governance Group. Personal use of email and use of strong passwords added.	Jo White
9.0	03/12/2018	Reviewed by Information Governance Group. No changes.	Jo White
10.0	14/01/2020	Reviewed by Information Governance Group. Advice on scanning devices added.	Jo White
11.0	09/02/2021	Reviewed by Information Governance Group. Added not using Derbyshire emails to sign up for services.	Jo White
12.0	08/03/2022	Reviewed by Information Governance Group. No changes.	Jo White
13.0	11/04/2023	Reviewed by Information Governance Group. No changes.	Jo White
14.0	14/05/2024	Reviewed by Information Governance Group. No changes.	Jo White

This document has been prepared using the following ISO27001:2022 standard controls as reference:

ISO control A.5.10-Acceptable use of assets
ISO control A.5.17-Use of secret authentication information
ISO control A.5.37-Documented operating procedures
ISO control A.6.3-Information security awareness, education and training
ISO control A.6.4-Disciplinary process
ISO control A.6.8-Reporting information security events/weaknesses
ISO control A.7.7-Clear desk and clear screen policy
ISO control A.8.1-Unattended user equipment
ISO control A.8.19-Installation of software on operational systems

2 Introduction

Derbyshire County Council provides many essential services and business functions which rely on ICT technology resources. The use of ICT resources must be in line with good professional working practices, procedures and must ensure the security and integrity of all Council information and data.

3 Purpose

The purpose of this policy is to establish how the Council's ICT facilities and resources must be used.

4 Scope

The scope of this policy extends to all departments, employees, elected members, contractors, vendors, volunteers and partner agencies (including schools and academies) who use/access the Council's ICT facilities.

5 Policy Statement

5.1 Information Handling

Hard copy documents and other media containing Council information assets as defined in the Information Asset Management Policy must be classified and handled in accordance with the Information Classification Handling Policy and Safe Haven Guidance

5.2 Computer Use

All users of Council Computers must ensure at all times that:

- They do not attempt to access personal data unless there is a valid business need that is appropriate to their job role.
- They do not attempt to compromise or gain unauthorised access to the Council's IT systems, telephony or network or prevent legitimate access to it.
- Authorisation has been provided to use the ICT facilities with a Domain username and password provided by Digital ServicesCT Service
- User and System account logon passwords are kept private and not shared, displayed or communicated to anyone who does not have a legitimate right to that information
- Council information and data is not permanently saved to local hard drives including PCs and laptops – in the event of the Council network being unavailable, advice should be sought from Digital Services.
- Data should only be saved on to a Council PC or laptop's hard drive as a last resort. As soon as possible the data should be copied to the appropriate storage location and deleted from the hard drive.
- Data and Information saved to portable devices via a PC is only copied to a Council approved portable device which is encrypted in accordance with the Council's Encryption & Cryptographic Controls Policy: Encryption Policy
- Where data is saved to a portable handheld scanning device, the images should be saved on to the Council's network as soon as practicable with the data then deleted immediately from the scanning device.

N.B - Mobile computing devices such as digital cameras and digital dictation devices etc., must not be treated as data storage devices – however, the Council accepts that photographs/audio files for Council purposes can also be classed as data and recommends that any photographs/audio files taken are removed from the device(s) and stored on the Council network as soon as possible. Unless for work purposes, if fitted with a geotagging (location identification) feature, this should be switched off.

- Screens/computers are locked by users when away from the computer
- Council computer equipment, such as desktops, (with the exception of laptop and other portable devices authorised for mobile use) are not removed from their location without line management and/or approval from Digital Services.
- Unauthorised, non-standard equipment is not connected to a computer in any way.
- Software is not installed on the Council's IT computer equipment by unauthorised staff (authorised access may include specific duties requiring staff to have administrative access in order to carry out certain job functions) – any software installed must be (or going through the process of being) placed on the approved software list
- Council's ICT equipment must not be used to store any personal data such as wedding photos, CV's, music files etc.
- Computers are not mishandled, wilfully damaged or tampered with in any way – this includes taking off the PC/laptop case cover, or removing of any screws or fixings
- Any suspicious or unknown equipment near or around PCs/laptops is reported to Digital Servicese.
- Computers should be logged off and shut down when not in use for extended periods (i.e. overnight) and monitors are powered off.
- Personal cloud/internet based IT facilities (e.g. Dropbox etc) are not used to store work related information.

5.3 Internet and Email Use

INTERNET

- Personal use of the Internet is allowed but not during working hours. You can use the Internet before you start work, during your lunchtime, or after work.
- The Council has in place a process to block categories of internet sites and individual sites if it is deemed appropriate.
- If you use the Internet to buy goods or services, the County Council will not accept liability for default of payment or for security of any personal information you provide.
- Personal goods must not be delivered to a County Council address.
- Downloading of video, music files, games, software files and other computer programs - for non-work related purposes - is strictly prohibited. These types of files consume large quantities of storage space on the system (and can slow it down considerably) and may violate copyright laws.

Many Internet sites that contain unacceptable content are blocked automatically by the Council's systems. However, it is not possible to block all "unacceptable" sites electronically. You must not therefore deliberately view, copy or circulate any material that:

- Is sexually explicit or obscene
- Is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- Contains material the possession of which would constitute a criminal offence
- Promotes any form of criminal activity
- Contains images, cartoons or jokes that will cause offence

Derbyshire County Council records the details of all Internet traffic. This is to protect the Council and its employees from security breaches, including hacking and to ensure that 'unacceptable' sites are not being visited.

EMAIL

Personal use of Council email systems is not permitted at any time. You must not use your Derbyshire.gov.uk email address to register for services, software or facilities that do not relate to your role with the Council.

It is inappropriate to use your Derbyshire.gov.uk email address for personal use as it may give the impression that any business is on behalf of the Council.
You must not use the email system in any way that is insulting or offensive. You must not deliberately view, copy or circulate any material that:

- Is a sexually explicit or obscene
- Is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- Contains material the possession of which would constitute a criminal offence
- Promotes any form of criminal activity
- Contains unwelcome propositions
- Involves gambling, multi-player games or soliciting for personal gain or profit
- Contains images, cartoons or jokes that will cause offence
- Appears to be a chain letter
- Brings the Council in to disrepute or exposes it to legal action

More information is available in the Council's Internet and Email Acceptable Use Policy: Internet and Email Acceptable Use Policy

The Council routinely produces monitoring information which summarises email use and may lead to further investigation being undertaken.

5.4 Security
The Council's computer systems are under continuous threat from hackers, virus/malware infections, data and equipment theft. The Council must remain vigilant at all times in order to safeguard information and data and to protect the security and integrity of all ICT systems.

Users of all Council computers and devices must ensure that:

- Computers/devices are not given to any unauthorised persons for safe keeping
- Computers/devices are not left discarded or unattended in public places
- All portable mobile computing devices and other IT equipment should not be left unattended in any vehicle at any time - further information is available from the Council's Risk and Insurance manager:
- Computers/devices must be adequately protected from physical damage
- Computers/devices are not hired, lent or given out without authorisation from Digital Services.
- All Computers/devices which are no longer required or which have reached the end of useful life must be returned via the line manager to Digital Services to be disposed of through the Council's ICT disposal procedure.
- Strong passwords are used to access the Council's computers and systems. Advice on creating strong passwords is available using the following link: Password Policy

5.5 Antivirus

Any warnings visible on screen from the Council's Antivirus/Antimalware software about identified/detected threats from viruses/malware should be reported to the Digital Services Service Desk immediately and recorded as a security incident via the Council's Security Incident Management Policy and Procedures which can be found using the link below:

Security Incident Procedures

5.6 Personal Devices

Personal devices which are not the property of the Council, including mobile phones, PDAs, digital pens etc., must not be connected to any Council computer without approval from Digital Services or used to record or capture information relating to the Council and its services.

6 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council's security procedures and policies.
All Council employees, elected members, partner agencies, contractors, volunteers and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

All users of the Council's ICT facilities must comply with the Council's Information Security Policy which can be found using the link below:
Information Security Policy

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.