
# ICT Security Awareness Procedures

## 1 Version History details and author

| | | | |
|---|---|---|---|
| 1.0 | 21/12/2010 | Completed for distribution | Jo White |
| 1.0 | 25/01/2011 | Agreed by Information Governance Group | Jo White |
| 2.0 | 29/02/2012 | Reviewed by Information Governance Group | Jo White |
| 3.0 | 27/03/2013 | Reviewed by Information Governance Group | Jo White |
| 4.0 | 19/05/2014 | Reviewed by Information Governance Group | Jo White |
| 5.0 | 13/07/2015 | Reviewed by Information Governance Group. | Jo White |
| 6.0 | 12/09/2016 | Reviewed by Information Governance Group. Changes to policy names. | Jo White |
| 7.0 | 09/10/2017 | Reviewed by Information Governance Group. GDPR added. | Jo White |
| 8.0 | 05/11/2018 | Reviewed by Information Governance Group. Frameworki changed to Mosaic. | Jo White |
| 9.0 | 14/01/2020 | Reviewed by Information Governance Group. GCSx reference removed. | Jo White |
| 10.0 | 09/02/2021 | Reviewed by Information Governance Group. No changes. | Jo White |
| 11.0 | 09/02/2022 | Reviewed by Information Governance Group. No changes. | Jo White |
| 12.0 | 11/04/2023 | Reviewed by Information Governance Group. No changes. | Jo White |
| 13.0 | 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:**

A.5.2 - Information security roles and responsibilities
A.5.3 - Segregation of duties
A.5.4 - Management responsibilities
A.5.16 – Identity Management
A.5.18 – Access rights
A.5.36 - Compliance with policies, rules and standards for information security
A.6.3 - Information security awareness, education and training
A.6.4 - Disciplinary process
A.6.5 – Responsibilities after termination or change of employment
A.8.2 – Privileged access rights

## 2 Introduction

It is vital for the protection of information and systems that Council employees, elected members, contractors, temporary staff, partner organisations and other authorised users having access to Derbyshire County Council systems and equipment are aware of and understand how their actions may affect the security of information. Compliance by users with ICT policies and procedures should result in individuals being made aware of their responsibilities and the consequences of their actions. This will reduce the risk of information loss, leakage or exposure through inadvertent or deliberate actions when utilising Council facilities and systems.

For the purposes of this document, it should be noted that future references to 'staff' and authorised ICT users will include members of the following groups:-

- All parties who have access to, or use of ICT systems and information belonging to, or under the control of, Derbyshire County Council including:
    - Council employees
    - Elected Members
    - Third Parties
    - Full and part-time staff
    - Temporary staff
    - Agency staff
    - Partner organisations, including Schools and Academies
    - Members of the public
    - Volunteers
    - Any other party utilising Council ICT resources

## 3 Purpose

The purpose of these procedures is to ensure the link between managers and staff and authorised ICT users with regard to ICT security is observed and understood. To ensure that security of information and systems is given due importance, it is essential that staff and authorised ICT users have the knowledge that policies exist and they are understood and adhered to.

## 4 Scope

The scope of these procedures includes all staff and authorised ICT users who have access to information and ICT systems. These procedures apply throughout the information lifecycle from acquisition / creation, through to utilisation, storage and disposal.

## 5 Responsibilities

Directors are responsible for ensuring that staff and authorised ICT users and managers are aware of security policies and that they are observed. Managers need to be aware that they have a responsibility to ensure that staff and authorised ICT users have the relevant knowledge concerning security of information and systems which they use. Designated owners of systems who have responsibility for the management of ICT systems and inherent information, need to ensure that staff and authorised ICT users have been made aware of their responsibilities regarding information security.

## 6 Procedure statement

Corporate induction programmes, eLearning, line manager training and specific training and awareness programmes should be undertaken by staff and authorised ICT users to enable them to be aware of their responsibilities towards information security. To evidence participation and completion of any induction training it is important that the employee signs (either electronically or manually) to confirm their awareness and understanding of the training received.

Education and awareness should include:-

- The benefits to both the Council and User of ICT security awareness
- The reasons why misuse and/or a breach of the guidelines can be so damaging and/or a significant issue for the council.
- The types of behaviour expected and the types of behaviour that are not acceptable which may result in disciplinary action.
- That authorisation is required to be able to access ICT systems and/or information.
- That any use of systems or access to information is carried out within acceptable boundaries as included in specific acceptable usage policies or the set of ICT security policies as a whole.
- That systems are predominantly for work use and any personal use should not interfere with an employee's ability to undertake their duties or be utilised during an individual's working day.
- That employees' usage of systems will be regularly monitored and where a potential breach of policy is noted, it is reported to the appropriate senior manager.
- That specific policies and procedures should be observed.
- That access to information and systems is a part of security and physical access to buildings and equipment also forms a part of the sphere of ICT security.
- That due consideration is applied to the sharing of information between internal departments/public/suppliers/contractors and partners to ensure that compliance with ICT policies and legal and contractual obligations are met.

In addition to new staff and authorised ICT users receiving ICT security awareness training as part of their induction to the Council, other ICT policies will have dedicated eLearning modules and these should be undertaken. It is part of a manager's responsibilities to ensure that all relevant training has been identified and is completed by staff and authorised ICT users as and when required, for example, when using new or upgraded systems/equipment.

Some ICT systems (e.g., Mosaic), enable access to confidential and/or 'sensitive' information thus background verification of potential or existing employees, contractors, temporary staff and authorised ICT users or third parties may need to be

undertaken in accordance with the security requirements of the ICT systems which are to be used.

Prior to use of any systems or equipment both the manager and the employee will need to ensure that the correct levels of individual system security/access and equipment are being used.

On termination or change of a contract or employment, staff and authorised ICT users should have access to Derbyshire County Council systems/equipment reviewed/removed and be made aware that their obligations to the security of information still apply.

## 7 Compliance with legal and contractual obligations

Derbyshire County Council is obliged to abide by all UK legislation regarding information security including:

- The Data Protection Act (2018)
- UK General Data Protection Regulation (2018)
- The Freedom of Information Act (2000)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- The Copyright, Designs and Patents Act (1988).
- The Regulation of Investigatory Powers Act (2000)
- The Electronic Communications Act (2000)
- Privacy and Electronic Communications Regulations (2003)

Derbyshire County Council must also comply with any contractual requirements, standards and principles required to maintain the business functions of the Council including:

- Protection of intellectual property rights;
- Protection of the authority's records;
- Compliance checking and audit procedures;
- Prevention of facilities misuse and fraud;
- Relevant codes of connection to third party networks and services.

In order to enable the Council to comply with its obligations relating to information security referred to above it will be necessary for staff and authorised ICT users to be made aware of and adhere to all Council policies pertaining to the use of ICT systems and information in general. Ensuring employees are aware of the policies will be the responsibility of managers but will be achieved through a combination of measures such as; induction, eLearning, as part of logon procedures whereby policies are required to be read and accepted.

## 8 Compliance with Council ICT policies

Several Council non-ICT and ICT specific policies need to be considered as relevant to the sphere of human resources and security awareness.
These include:-

- Security Incident Management Policy and Procedures
- Safe Haven guidance
- Information Security policy

- Wireless Network policy
- Password policy
- Secure Desk Policy
- Internet, Email and Social Media Acceptable Use policy
- Encryption & Cryptographic Controls policy
- ICT Acceptable Use policy
- Public Internet Access policy
- Operational Management policy

To achieve compliance with the above, managers should ensure that all staff and authorised ICT users have suitable access to the policies and undergo any further necessary training.

## 9 Incidents and Breaches of policy

Failure to observe these procedures could lead to inadvertent or deliberate breaches of security. This in turn could damage the reputation of Derbyshire County Council and incur financial penalties. Further to this, citizens' information and trust may be compromised resulting in detrimental effects to both the citizen and Council. The breach may also result in the relevant member of staff and authorised ICT users being dealt with under the disciplinary process.

All possible breaches of security should be handled in accordance with the specific policy and the 'Security incident management policy and procedures'.

This outlines the ways of identifying possible breaches, the available reporting mechanism, what sort of incidents need to be reported and for what reasons.

The range of incidents which will require security awareness procedures include:

- Computers left unlocked when unattended
- Password disclosures and use of weak passwords
- Virus warnings/alerts
- Media loss
- Data loss/disclosure
- Personal information abuse
- Physical security
- Missing correspondence
- Found correspondence/media
- Loss or theft of IT/information
- Misuse if IT equipment/facilities
- Storage of unauthorised material on council equipment

Resolution of incidents may require further investigation, training, manager's intervention and may involve disciplinary procedures.

If there is any doubt concerning a possible incident/breach then it should be referred to an individual's line manager or logged as an incident via the Council's Security Incident Policy and Procedures

***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.***