Encryption & Cryptographic Controls Policy

1 Version History details and author

1.0	22/10/2010	Completed for distribution	Jo White
1.0	24/11/2010	Approved by Information Governance Group	Jo White
2.0	26/05/2011	Reviewed by Information Governance Group	Jo White
3.0	25/10/2011	Reviewed by Information Governance Group	Jo White
4.0	28/11/2012	Reviewed by Information Governance Group	Jo White
5.0	13/01/2014	Reviewed by Information Governance Group	Jo White
6.0	09/02/2015	Reviewed by Information Governance Group.	Jo White
7.0	11/05/2015	Reviewed by Information Governance Group. Renamed from Encryption Policy.	Jo White
8.0	13/06/2016	Reviewed by Information Governance Group.	Jo White
9.0	10/07/2017	Reviewed by Information Governance Group. Transformation changed to ICT. Moving of documents from removable storage to network added.	Jo White
10.0	06/08/2018	Reviewed by Information Governance Group. Clarification of TPM chip added.	Jo White
11.0	06/11/2019	Reviewed by Information Governance Group. Policy rewritten to describe how to encrypt.	Jo White
12.0	14/04/2020	Reviewed by Information Governance Group. Section 4.4 updated to include Service Desk access to bit-locker keys and updated process for bit-locker keys.	Jo White
13.0	09/03/2021	Reviewed by Information Governance Group. MFA removed and added to security objectives.	Jo White
14.0	08/03/2022	Reviewed by Information Governance Group. No changes.	Jo White
15.0	11/04/2023	Reviewed by Information Governance Group. Links corrected.	Jo White
16.0	11/06/2024	Reviewed by Information Governance Group. Agency staff added. ISO27001 controls updated.	Jo White

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

A.5.10 – Acceptable use of information and other associated assets
A.5.12 - Classification of information
A.5.13 - Labelling of information
A.5.14 - Information transfer
A.5.20 - Addressing information security within supplier agreements
A.5.31 – Legal, statutory, regulatory and contractual requirements
A.7.10 – Storage media
A.8.1 – User endpoint devices
A.8.20 – Networks security
A.8.24 – Use of cryptography

2 Introduction

The protection of electronic information and systems continues to be a prime focus for the Council. Protecting personally identifiable, business critical information and the integrity of the Council's computer network is of paramount importance.
A secure, robust ICT infrastructure, along with appropriate policies and procedures will help to ensure that all necessary steps have been taken to protect the confidentiality, integrity and availability of information, systems and data.

The General Data Protection Regulation (GDPR) and The Data Protection Act 2018 require the Council to implement appropriate technical and organisational measures to ensure that personal data is processed securely. Article 32 of the GDPR includes encryption as an example of an appropriate technical measure. Encryption is a widely available measure with relatively low costs of implementation and helps to ensure that appropriate controls are used.

The Information Commissioner's Office (ICO) has considered encryption to be an 'appropriate technical measure' for a number of years. In cases where data has been lost or unlawfully accessed and encryption has not been used, the ICO will consider taking appropriate regulatory action.

3 Purpose

The purpose of this policy is to establish the methods by which the Council takes in the application of encryption and cryptographic control technologies - ensuring that data is protected however and wherever it is processed, stored or communicated and that the Council's ICT computer network and devices are appropriately secured from unauthorised access and compromise.

4 Scope

This policy applies to the use and configuration of encryption applied to Council ICT systems, computing devices, communication technologies and services - including all employees, elected members, contractors, volunteers, vendors, apprenticeships, student/work experience placements and partner agencies who have access to these systems, equipment and devices.

5 Policy Statement

Encryption works by converting data to make it unreadable and inaccessible to unauthorised individuals. The only way to read the encrypted data is by using a decryption key. The Council uses encryption to:

- Secure information and data while stored, processed and handled
- Protect user credentials (passwords/logons),
- Enable secure communications and connections
- Enable verification, authentication, identification and validation.
- Secure ad-hoc internet/networked connections between ICT systems and devices.

Computers

Laptops are the most widely used computing devices across the Council. Despite the Council's policy that no data should be stored on these devices, there continue to be situations and events which may cause data to be stored whether knowingly or unwittingly by users. The portable nature of laptops increases the risk of theft and/or loss but more importantly, the loss or disclosure of data itself. The most effective and

appropriate way of addressing these risks is by protecting these devices with encryption using the following methods:

- Operating system images installed on desktop and laptop computers must be configured with a minimum of **AES 128 bit** (Advanced Encryption Standard) using symmetric-key encryption with a 128 bit key.
- Encryption employed on desktop and laptop computers must allow for a random cryptographic key to be generated and for the relevant key to be stored in the Council's Active Directory (AD).
- During the build process for desktops and laptops, processes must be in place to check the make and model of computers to verify they have a Trusted Platform Module (TPM) chip on board. The build process should enable the TPM function and start the encryption process accordingly:
    - A random key is generated by the TPM chip
    - Cryptographic keys are written back to Active Directory.
    - If the Council's computer network becomes unavailable (preventing keys being stored in AD) remediation techniques must be in place to ensure that these computers are identified and methods are used to initiate the storing of cryptographic keys for these computers in AD.
    - If a desktop or laptop computer doesn't have a TPM chip on-board, the build should be allowed to continue the encryption process, with the use of a USB key on which the encryption Key can be created.
- If immediate writing of cryptographic keys to the AD is not possible, allowance is made to write the key to USB media which must be stored appropriately following the process.
- All desktop and laptop computers must be updated with the latest security and OS patches as these updates may include security patches to flaws or vulnerabilities discovered in the encryption software.
- All desktops and laptop images must ensure the continued encryption of hard drives including timely cryptographic key recovery methods as required.

MOBILE DEVICES AND PORTABLE STORAGE MEDIA

Increasingly, mobile phones are being used by Council employees. This increases the likelihood of data exposure and despite Council policy that no data should be stored on these devices and the application of technical controls to help prevent this, it is inevitable that unforeseen events and actions may cause some restricted type data to be stored on these devices.
The Council has taken the following measures in order to address this:

Mobile Devices

- All Council provided mobile phones must be configured to force the use of a pin code lock which includes a minimum of eight characters. While the use of a PIN alone to secure a mobile phone does not constitute encryption, it does play a vital role in supporting mobile device encryption.
- Council managed mobile Apps which are authorised for use and which may process or handle personally identifiable data must use encryption to protect data.
- Council authorised Apps must use secure encrypted communication protocols such as HTTPS/TLS1.2 (or higher) when communicating over the internet or any other unspecified network connection.

Portable Storage Media

Where required, the Council provides encrypted USB data sticks. These storage devices are for the temporary storage of data only.
The Council allows the use of council issued USB data sticks (and similar storage devices) under the following conditions:

- Users must set a password for accessing the device.
- The password for encrypted, portable devices must be in accordance with the Council's password policy.
- Using the portable device on any other computer after being encrypted will require a password in order to access it.
- Council data stored on encrypted USB sticks (or similar storage devices) must be transferred to an appropriate, secure area on the Council's computer network as soon as possible - Council data should NOT remain on the data stick.
- In the event that local procedures for the creation of encryption passwords have not been followed, employees may be asked to provide details of encryption passwords used on all such portable devices – however, under no circumstances should **network** or other **IT system** passwords be disclosed to anyone including Digital Services**.**

Other portable USB devices include mobile phones, cameras etc. These other devices should not be used to store Council data on the device. Data collected as part of their use should be transferred to the appropriate system at the earliest opportunity.

Personal storage media and equipment must NOT be connected to the Council's network for non work purposes and must NOT be used to store Council data.

If clarification is needed as to the recommended USB data storage devices allowed for use, the Digital Services Service Desk should be contacted.

The Digital Services Service Desk will advise on the best method to encrypt individual files.

INTERNET AND EMAIL

Internet

Increasingly, internet websites have adopted the secure, encrypted connection protocol HTTPS in combination with TLS as default. The main search engines such as Google, Bing etc., now use an encrypted connection as standard, however, not all sites have a secure connection as yet. This is something to bear in mind when using the internet for Council business. The Council's public facing website derbyshire.gov.uk uses HTTPS – helping to protect users of provided services such as the Council's recruitment website, by encrypting connections which in turn, helps to protect passwords and data while travelling across the internet.

Email

All Council internal emails are encrypted i.e. derbyshire.gov.uk to derbyshire.gov.uk Emails sent from the Council to external recipients do not remain encrypted. The Council provides other methods to send secure, encrypted email to external recipients. Methods of sending encrypted emails vary depending on where the email is being sent to. Emails containing personal or sensitive information MUST be sent by a secure email system. The Council has established various methods of sending encrypted emails.

The Council's **Secure Email Policy** describes these methods in detail: https://staff.derbyshire.gov.uk/sharing-info

CRYPTOGRAPHIC KEYS

Cryptographic keys are required to access data and systems which utilise encryption. The Council takes the following approach in the management of these keys:

- Access to cryptographic keys in Active Directory must be restricted to authorised staff only, this is currently limited to Digital Services Data Centre Team and Digital Services Service Desk.
- Procedures must be in place to ensure that requests for cryptographic keys can be appropriately authorised, provided in a timely manner and appropriately recorded.
- If a cryptographic key is provided for recovering access to a computer, the existing key must be revoked, and a new key must be generated to prevent data leakage and use of such keys is recorded.
- Cryptographic keys must be securely managed and protected though their whole lifecycle from initial generation and storage to archiving, retrieving, distributing, retiring and eventual destruction.
- Cryptographic algorithms, key lengths and use must be in accordance with all relevant Council policies, procedures and in accordance with professional best practices.
- Cryptographic keys must be protected though their whole lifecycle against modification, loss, unauthorised access/use or disclosure.
- Equipment used to generate, store and archive keys must be physically protected using appropriate, secure access controls.
- Awareness of encryption/decryption passwords for devices, media or systems must be limited to authorised personnel only.
- In the event of a cryptographic key being compromised, the existing key must be revoked and a new key (or key pair) must be generated.

N.B.
The loss of a decryption key could cause data to become inaccessible. Depending on the circumstances, loss of a decryption key could constitute 'accidental loss, destruction or damage' to personal data and would therefore be a contravention of the GDPR's security principle. Additionally, if data cannot be restored, this may also constitute a personal data breach due to a lack of availability.

6 Responsibilities

The Council has a responsibility to provide its employees with the appropriate secure storage mechanisms, procedures, devices and software for the secure handling, storage and retrieval of all electronic data held by the Council. The use of portable devices may be subject to random periodic review by the Council to ensure compliance with the encryption policy.

All Council employees, elected members, volunteers, agency staff, partner agencies, contractors and vendors have a duty to abide by all Council policies and procedures to ensure the safe, secure handling of all electronic data.

7 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, volunteers, partner agencies, contractors 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.

In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Council's ICT systems or network results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under the Council's disciplinary process.

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.