Data Protection & Storage Media Handling Procedures

1 Version History details and author

1.0	21/04/2011	Completed for distribution	Jo White
1.0	26/05/2011	Approved by Information Governance Group	Jo White
2.0	22/06/2012	Reviewed by Information Governance Group. Approved by email as meeting was cancelled.	Jo White
3.0	31/07/2013	Reviewed by Information Governance Group. Word corrections. Data added after information under 6, 7, 9, 10 and 12.	Jo White
4.0	08/09/2014	Reviewed by Information Governance Group	Jo White
5.0	16/11/2015	Reviewed by Information Governance Group.	Jo White
6.0	05/12/2016	Reviewed by Information Governance Group. Encryption Policy name update.	Jo White
7.0	08/01/2018	Reviewed by Information Governance Group. Transformation changed to ICT.	Jo White
8.0	03/02/2019	Reviewed by Information Governance Group. No changes.	Jo White
9.0	03/03/2020	Reviewed by Information Governance Group. Links updated.	Jo White
10.0	13/04/2021	Reviewed by Information Governance Group. No changes.	Jo White
11.0	10/05/2022	Reviewed by Information Governance Group. No changes.	Jo White
12.0	06/06/2023	Reviewed by Information Governance Group. Information sharing agreements updated.	Jo White
13.0	13/08/2024	Reviewed by Information Governance Group. ICT changed to Digital.	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 > 5.13 – Classification and Labelling of Information
A.5.14 – Information transfer
A.5.34 - Privacy and protection of PII
A.6.6 - Confidentiality or non-disclosure agreements
A.7.9 – Security of assets off-premises
A.7.10 – Storage media
A.8.24 – Use of Cryptography

2 Introduction

Derbyshire County Council is required at all times to comply with the Data Protection Act 2018 to ensure all data and information it holds is protected. All methods and mechanisms which are used to store, retrieve and/or disseminate data must also satisfy the requirements of the Data Protection Act 2018 and all processes and procedures should be carried out in line with professional best practice.

Storage Media is used to both store data and to transport it from one location to another. In order to ensure the protection of data, all media must be safeguarded against disclosure, theft, or damage. Risk mitigation controls which include appropriate media labelling, storage, safe transportation, disposal and handling are necessary and vital to protect all forms of media used for the storage of data.

The Council's Safe Haven Guidance provides clear and comprehensive information on many aspects of the safety and security of data and information. This procedure is intended to provide more specific guidance on Data Protection and Media Handling.

3 Procedures

The following is provided for guidance to enable adherence to the security and protection of data and the handling of related media:

1. Data, information and media must only be accessed, processed and transmitted as and when required by authorised persons for Council business purposes and must not be accessed, viewed or processed in any way for casual or personal use

2. Where the Council shares personal data with an external organisation, an Information Sharing Agreement is normally required. See the Information Sharing Policy and Guidance for details.

3. The Council provides a process by which requests may be made to the Digital Services Service Desk for data which needs to be encrypted on portable media such as laptops, memory sticks and DVDs/CDs. This will ensure that the security and integrity of data being delivered/transported to other Council locations, external organisations and partner agencies is maintained and cannot be intercepted/amended. Encryption levels of data on such media must be a minimum of 128bit AES - in line with the Council's Encryption and Cryptographic Controls Policy. Sensitive and personal data must not be faxed to an unsecured location under any circumstances (as per 'Sending faxes' advice contained with Safe Haven Guidance). All requests for encrypted media must be requested via the Digital Services Service Desk.

4. Formal Information Sharing/Exchange agreements must detail the responsibilities, technical and procedural control standards, liabilities and any special controls that may be required in order to ensure the secure information exchange through all communication methods

5. All information assets must be classified and appropriately marked to determine the level of security protection (including backup, storage, encryption,

maintenance, records and audit requirements) they are afforded based on risk assessments. More information on data backups is available in the Council's Information Backup and Restore Procedures

6. Paper files, removable media and other records or documents containing personal or sensitive information and data must be kept in secure environments in line with the Council's Safe Haven Guidance and Secure Desk Policy and not removed, transmitted, transferred or copied in any form (including physical transfer or electronic communications method) that, if loss or interception occurs, introduces an unacceptable risk of disclosure, theft, or damage to data and information. Link to Safe Haven Guidance and Secure Desk Policy: importance of information security

7. If media contains sensitive or personal information and data and you cannot physically secure your workspace or area, you must store any such media securely within a locked cupboard, drawer, office or other securely 'locked' environment

8. The use of courier contractors to transfer information/media is restricted to organisations and agencies with which the Council has formal contractual agreements

9. Personal or sensitive information and data held on, or transmitted between, electronic systems and the systems themselves, are protected by the implementation of procedural and technical controls that reduce risks of interception, unauthorised disclosure, loss or unauthorised alteration to acceptable levels as defined by the Council's Risk Management Strategy.

10. Personal or sensitive information and data is not transmitted via electronic messaging services including email and Electronic Data Interchange (EDI) systems unless appropriately protected and with the approval of Digital Services management and the Information Security Manager. The transmission of personal or sensitive information by SMS text and Instant Messaging services is not permitted under any circumstances

11. The retention of information must be defined by retention policies which meet the requirements of the Council, contract or UK legislation and appropriate procedures must be implemented to ensure that information is held securely and is safely retrievable on request

12. Sensitive or personal information and data held on any media must be physically destroyed when due for disposal or no longer required. Procedures for identifying media that requires secure disposal must be implemented and an audit trail of any media passed to external organisations must be maintained. Where specialised disposal techniques are required, media must only be passed to reputable organisations dealing with secure disposal of information with whom the Council has formal contractual agreements. Backup data/media no longer required must be disposed of securely and with due environmental consideration (WEEE Directive) – more information is available at disposing of information

13. All sensitive and personal information and data stored on portable media must be Council supplied media and encrypted in line with the Council's Encryption 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.