Secure File Transfer Policy

1 Version History details and author

1.0	22/04/2015	Completed for distribution	Jo White
2.0	13/07/2015	Approved by Information Governance Group.	Jo White
3.0	09/08/2016	Reviewed by Information Governance Group.	Jo White
4.0	09/10/2017	Reviewed by Information Governance Group. Transformation changed to ICT. Changes to Microsoft Encrypted email. Information about dealing with schools added.	Jo White
5.0	05/11/2018	Reviewed by Information Governance Group. Changes to GCSx use.	Jo White
6.0	18/12/2019	Reviewed by Information Governance Group. References to procedures removed. GCSx sections removed.	Jo White
7.0	12/01/2021	Reviewed by Information Governance Group. No changes.	Jo White
8.0	08/03/2022	Reviewed by Information Governance Group. Tidy up of terminology.	Jo White
9.0	11/04/2023	Reviewed by Information Governance Group. No changes.	Jo White
10.0	14/05/2024	Reviewed by Information Governance Group. TLS explanation added.	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.5.14 – Information transfer
A.5.28 - Collection of evidence
A.5.32 - Intellectual property rights
A.6.2 - Terms and conditions of employment
A.8.6 - Capacity management
A.8.15 - Logging

2 Introduction

Derbyshire County Council has complex involvements, both internally between departments and externally with partner services and agencies. Some of the fundamental functions of the Council rely on the safe and secure transfer of information between internal departments and external partners/agencies. The foundation of this transfer is based upon the available facilities that can be used in a timely and secure fashion, dependent upon the classification of the data in the transfer.

The secure file transfer facilities provide the appropriate mechanism by which the information, of any type or classification, can safely and securely by transferred as and when required within the Council and between external partners/agencies.

3 Purpose

The purpose of this policy is to define the requirements which ensure that the Council's critical or sensitive information is transferred/received using appropriate methods in accordance with the classification of the data. Appropriate security and controls provide protection against unauthorised access or damage to information both during transfer and on receipt.

This policy should be read in conjunction with the Information and Classification Handling Policy, Password Policy, Internet and Email Policies and Safe Haven Guidance.

4 Scope

The scope of this policy includes all persons/parties who have access to Council and or partners/agency information and ICT systems 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
- Any other party utilising Council ICT resources

5 Policy Statement

There are several factors that will influence the data sent/received and the facility used to transfer the files:-

- Classification
- Recipient/sender
- File size
- Access control

Any information not classified as Public must be transferred via a secure method.

Recipients/senders of certain types of files sent to certain recipients must be transferred via a specific method. This is particularly applicable to files being sent/received to/from government departments, agencies and national bodies.

Data should never be passed or transferred to employees/agencies/partners if that party is not authorised to view that information.

Files over certain sizes cannot be sent via secure email and should therefore be transferred by another Council agreed secure method.

There are several methods by which file transfer can take place. The classification of the data sent/received and to whom, will dictate which method is most appropriate:-

Standard Derbyshire County Council Email

1.Emails sent from one Derbyshire.gov.uk account to another Derbyshire.gov.uk account are encrypted and deemed secure for file transfer of any classification (public, controlled or restricted).

- When sending to a team/generic email account, it must be checked that all persons with access to the team email address are authorised to view any attached files.
- Delegate access should be reviewed to ensure delegates are authorised to view files. If delegate access is not authorised any email with attached files must be saved to a secure network location or EDRM.
- Emails classified as 'restricted' should not be sent to DCC distribution lists unless everyone in the distribution list is authorised to access information included in the email.

2. Emails sent from a Derbyshire.gov.uk email address to a non derbyshire.gov.uk email address, including derbyshire.sch.uk, are deemed secure if protected by Transport Layer Security (TLS). TLS will apply if the sender uses the default sensitivity setting, Controlled. TLS will not apply if the sender uses sensitivity settings to classify the message as Public. This method will successfully deliver the message to an email recipient in a domain that does not use TLS. However, such messages are deemed insecure because they do not stay within the Derbyshire email system and should only be used to transfer documents/files that are classified as 'Public'.

CJSM Email.

CJSM (Criminal Justice Secure eMail Service) is provided for criminal justice agencies and practitioners to communicate with each other. As a general rule it must only be used for purposes relating to the criminal justice service.

Microsoft 365 Encrypted email

This facility has been applied to all standard individual and generic derbyshire.gov.uk email accounts. This method can be used to send/receive files classified as controlled or restricted from external partners, agencies and individuals which cannot be contacted via CJSM email. The attached files on a single email must not exceed 13mb, unless by request to the Service Desk.

Cryptshare File sharing facility.

An externally hosted facility to securely share files with a user defined set of external parties. It can be used if files are too large to be sent via email or may need to be available over a specific period of time. It is available to be used through specific request to the Digital Services Service desk. Files of any classification can be shared

Children's Services Secure Document Transfer Portal on Derbyshire SchoolsNet website (i.e. Perspective Lite, Broadcast+ Module).

1. An externally hosted secure document transfer web portal for the Council's schools extranet i.e. Derbyshire SchoolsNet using a solution badged as **Broadcast+** for Council administrators as part of Nexus solution and **Perspective Life** for school administrators.
2. It can be used to transfer controlled/restricted documents by Council staff and teachers/staff members who have been assigned logon credentials to restricted access network folders on the system itself.

3. It is the primary method of secure document exchange between the Council and Derbyshire schools/academies (excluding independent schools) and should be considered first before adopting any other method of sharing confidential documents with Derbyshire schools/academies.
4. Contact Children's Services Management Information Team for further information.

6 Alternative methods.

Files which need to be shared with other external partners and individuals but cannot be transferred by any of the above methods may be transferred by methods specified in the Information Classification and Handling Policy

7 Further considerations:

It must be ensured that whichever method is used to send information, that only the correct recipient(s) receives that information, be that internally to the Council or externally.

A confidentiality clause or non-disclosure agreement should be in place to ensure the protection of information distributed to external agencies. Confidentiality clauses or non-disclosure agreements need to be regularly reviewed and documented.

Other than the above methods, any internet sites externally hosted, web based or unauthorised cloud based services, must not be used to transfer information, either as an email, an attachment or file.

The above methods must not be utilised for personal use and/or non-council purposes.

8 Breaches of Policy

If you feel you may have accidentally breached this policy, you should contact your line manager **immediately**, or, in their absence, a more senior manager who will record this information.

Breaches of this policy and/or security incidents can be defined as events which may have/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 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 employee then the matter may be dealt with under the 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.