Information Classification and Handling Policy and Procedures

1 Version History details and author

1.0	27/06/2013	Approved by Information Governance Group Jo White
2.0	31/07/2013	Approved by Information Governance Group Jo White
3.0	13/10/2014	Reviewed by Information Governance Group Jo White
4.0	11/05/2015	Reviewed by Information Governance Group. Classification for removable media added. Jo White
5.0	16/11/2015	Reviewed by Information Governance Group. Jo White
6.0	05/12/2016	Reviewed by Information Governance Group. No changes. Jo White
7.0	11/09/2017	Reviewed by Information Governance Group. Transformation changed to ICT. Controlled email allowed to be sent unencrypted to UK/EU. Jo White
8.0	08/10/2018	Reviewed by Information Governance Group. No changes. Jo White
9.0	06/11/2019	Reviewed by Information Governance Group. No changes. Jo White
10.0	08/12/2020	Reviewed by Information Governance Group. No changes. Jo White
11.0	07/12/2021	Reviewed by Information Governance Group. Policy and Procedures combined. Jo White
12.0	10/01/2023	Reviewed by Information Governance Group. Teams calls added to scope. Agency staff and cloud access incorporated. Jo White
13.0	13/02/2024	Reviewed by Information Governance Group. No changes. Jo White
14.0	11/03/2025	Reviewed by Information Governance Group. Family/Youth added to Court Proceedings. Jo Williams

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

A.5.12 - Classification of information
A.5.13 – Labelling of Information
A.5.33 - Protection of Records

2 Introduction

Derbyshire County Council is committed to the protection of all information regardless of the form it takes. Ensuring a consistent approach to the management and protection of information assets requires an information labelling and handling methodology with clearly defined procedures.

For the purpose of this policy, an asset is defined as functions, equipment and information regardless of the form it takes, and which is deemed to have value to the organisation.

3 Purpose

The purpose of this policy is to establish the key classification and handling principles for the protection of the Council's information assets, which should only be available to individuals who have a legitimate need to access them.

4 Scope

The scope of this policy extends to all information assets which have been deemed to have a security classification applied to them. Leaflets, information packs and blank application forms are excluded. The information covered in this policy includes, but is not limited to, information that is either stored or shared via any means. This includes electronic information, information on paper and information shared orally or visually (e.g., telephone conversations or video conferencing including 'Teams' calls).

Information received from other organisations must be handled according to information sharing agreements (where they exist) and treated with the equivalent Council information classification level - unless specific handling instruction has been provided otherwise with the information.

5 Policy Statement

All Council information has a value to the organisation, however not all of the information has an equal value or requires the same level of protection. Being able to identify the value of information assets is key to understanding the level of protection required. Once the appropriate level of protection is identified, the appropriate control can be implemented to prevent loss, damage or compromise of the asset, disruption of business activities, and prevention of the compromise or theft of information and information processing facilities. Incorrect classification of assets may result in inadequate or incorrect controls being implemented to protect them, which in the case of over classification would incur additional costs to the Council.

6 Information Classification

All information assets will be classified into one of three categories. The information asset must be appropriately labelled to ensure that its classification is readily identifiable.

Document authors will need to ensure that classification status markings are applied to all documents by selecting the classification from the Sensitivity menu in M365 applications (Word, Excel. Email etc.) or applying this marking manually.

All information must be clearly marked with the appropriate classification as a minimum in the document header prior to printing. If the material is already printed or has not been word-processed, the marking 'PUBLIC', 'CONTROLLED' or 'RESTRICTED' as appropriate, must be written, at the top of every page as a minimum. Multiple page documents must be stapled together.

RESTRICTED

Information whose unauthorised disclosure (even within the organisation) could cause serious damage in terms of financial loss, legal action, loss of reputation, damage to individuals and/or compliance with the UK GDPR.

Access is restricted to personnel with specific roles and clearance or with statutory rights of access.

Examples:

- Adoption records.
- Child Protection records.
- Disciplinary records.
- Social Care files with local restrictions e.g., family members.
- Family/Youth Court Proceedings.
- Public Health data containing Patient Confidential Data.
- Audit Reports.
- Personal occupational health referrals and reports.
- Applications under RIPA and reports of the Commissioner.
- Certain Council exempt papers.

CONTROLLED

Information generally available to anyone within areas of the Council and which contains business value to the organisation, or which requires protection due to personal data.

Access is restricted to staff within the organisation in connection with their employment.

Examples:
- Social Care information not in Restricted.
- IT Procedures relating to the Data Centres, Network, Backups etc.
- Personnel files.
- My Plans.
- Contracts.
- Council exempt papers unless with a restricted section.
- Commercially sensitive files.
- Draft service plans.
- Restructuring documentation.
- Business Continuity Plans.

PUBLIC

Information that can be made available in the Public Domain and which would not cause damage or harm if released.

Access is not restricted.

Examples:
- Office opening times.
- Business numbers.
- Press releases.
- Policies & Procedures.
- Forms.
- Minutes other than exempt.
- Statistics & Performance Indicators.
- General recruitment information and terms of conditions of employment.

All information must be categorised using either '**PUBLIC**', '**CONTROLLED**' or '**RESTRICTED**' and must be labelled accordingly.

N.B. Where information is grouped together, the highest classification shall be applied to all information in the group.

Any information that is not specifically marked as being 'RESTRICTED' or 'CONTROLLED' will be deemed to be 'PUBLIC'. Therefore, the officer responsible for processing or handling information, particularly if consideration is being given as to whether it should be disclosed, **MUST** consider the content in determining how it should be processed and not rely on its classification under this policy. The labelling of

information does not override the Council's duties under the Data Protection Act, the UK GDPR, the Freedom of Information Act 2000 or the Environmental Information Regulations 2004.

Once an information asset (e.g., paper documents) ceases to be active and is transferred to the Derbyshire Record Office for permanent preservation, its classification status will be reviewed by departmental staff prior to transfer.

Where an individual document is being created, the document author must ensure the appropriate classification markings are applied - preferably to the header of the document.

The classification status of information may change over time (i.e., a document may have a 'Restricted' classification early in its lifecycle, but this may be downgraded to a 'Controlled' classification as time progresses). Regular reviews of classifications are therefore vital.

7 Information Handling

The following table provides electronic information handling guidance for the classifications. All hardcopy information needs to be stored and handled as specified below.

Removable media such as CDs or DVDs, USB data sticks etc. used to store Council information must always be classified as 'RESTRICTED' and do not require individual labelling or marking.

Actions and Permitted Classifications

View/process on internal network within organisation's premises – Public, Controlled, Restricted
View/process on internal network away from organisation's premises – Public, Controlled, Restricted
View/process away from internal network – Public
View/process across encrypted remote access – Public, Controlled, Restricted
View/process across unencrypted remote access – Public

8 Information Transmission

The following table provides guidelines on methods of information transmission for classifications as described in **section 4.1.**

Transmission Method

By internal mail within the same building – Public, Controlled, Restricted.
By internal mail between buildings – Public, Controlled, Restricted.
By standard post to UK/EEA destinations* - Public, Controlled, Restricted.
By recorded/special delivery to UK/EEA destinations – Public, Controlled, Restricted.
By courier to UK/EEA destinations – Public, Controlled, Restricted.
By facsimile to UK/EEA destinations – Public, Controlled, Restricted.
By encrypted email internal to the organisation** - Public, Controlled, Restricted.
By unencrypted email external to Derbyshire County Council to UK/EEA destinations – Public, Controlled.
By encrypted email external to Derbyshire County Council to UK/EEA destinations – Public, Controlled, Restricted.
Across secure transmission link i.e. VPN – Public, Controlled, Restricted.
By encrypted media (e.g. encrypted data sticks) – Public, Controlled, Restricted.
Telephone & Video Conferences – Public, Controlled (provided the caller has been identified and is entitled to receive the information and the call is not in a public area), Restricted (provided the caller has been identified and is entitled to receive the information and the call is not in a public area).
Text/Multimedia/Instant Messaging – Public.

* consideration should be given to whether special or recorded delivery is required.
** Derbyshire County Council email is encrypted (internally) in transit only. Delegates to mailboxes must be deemed to have the same access rights to the information held in the email as the mailbox owner. The mailbox owner is responsible for reviewing who has delegate access to their mailbox.
All Derbyshire County Council emails will be classed as **'CONTROLLED'.** The status may be changed to **'PUBLIC'** or **'RESTRICTED'** by the user.

Whenever data classified higher than 'Public' is to be transmitted to a destination **outside** of the European Economic Area (EEA), advice must be sought from the Council's Information Security & Governance Manager.

For transporting of any kind of information, there are controls which must be used in order to avoid the loss of media in transit or its misuse, and to protect it from unauthorised access or corruption:

- **RESTRICTED** information must be encrypted at all times when emailed or electronically transferred outside of the Derbyshire County Council network.
- **CONTROLLED** information must be encrypted at all times when emailed or electronically transferred outside of the Derbyshire County Council network.
- **PUBLIC** information requires no secure method of transportation

Protectively marked physical information must be transferred in sealed packaging. A trusted and authorised courier service must always be used. The Council's Safe Haven guidance details the processes for sending and receiving physical mail securely for both internal and external posting.

9 Information Storage

Information should be stored in accordance with contractual or legislative requirements and in a manner commensurate to its classification, as follows:

- **PUBLIC**:
  Does not require any access restrictions or specific safe storage.

- **CONTROLLED**:
  If information is removed from the Council for use by home-workers it must not be left unsecured in employees' vehicles (including in the boot overnight) or left in public places. Information and data must be stored wherever possible, in a lockable area when at the employee's home that cannot be accessed by any unauthorised person, including family members.

- **RESTRICTED**:
  This information is sensitive information of which access must be restricted to authorised individuals only - securely locked away at the end of each working day or when no longer needed. This applies regardless of the format which this information is held on e.g., paper, disk, files, tapes, faxes, post.

When stored in an electronic format, information must be protected by the use of both technical and physical access controls. The following must be in place for:

Restricted Information stored on servers:

- Servers must be located within secure rooms at Derbyshire County Council premises or within an approved supplier or cloud hosting environment. In all instances access must be restricted to authorised personnel only.
- Logical access controls must be used with authorised user ID and strong passwords.
- Data stored in defined areas of the network must only be available to those authorised users with a need-to-know
- Encryption must be employed wherever possible

Restricted Information processed on laptops:

- Laptop hard drives must have full disk encryption applied with a minimum of 128bit AES (as defined in the Encryption and Cryptographic Controls Policy)
- Only authorised users with Council network domain credentials are authorised to use laptops. 'Local' accounts are not permitted for general use

- Authorised users viewing restricted data on a computer screen must observe the Council's Safe Haven guidance with particular attention to preventing the possibility of 'Shoulder Surfing' or casual viewing by unauthorised people
- Data must be moved from the laptop to a secure area on the Council's network as soon as possible

Restricted Information held in hard copy:

- Within Council buildings must be locked away in secure storage
- Within Employees homes must be stored, wherever possible, in a lockable area that cannot be accessed by any unauthorised person, including family members
- At premises other than Council locations if used for reference by third parties and/or other agencies, must remain within the Council's employee line of sight/possession and only made available to those with a need-to-know before retrieval
- In transit must not be left unsecured in employees' vehicles or left in public places.
- Information held on portable (removable) media, such as (but not limited to) CD, DVD, USB and Tape (including backup media) must have protection and encryption measures in order to protect against loss, theft, unauthorised access and unauthorised disclosure or;
    - When stored in another form, must be stored only in a locked drawer or room or an area where access control measures exist to provide adequate protection and prevent unauthorised access by members of the public, visitors, or other persons without a need-to-know.
    - When verbally discussing RESTRICTED information in public places or on public transport (including mobile phone conversations) care should also be taken in order that the conversation is not overheard. These rules also apply to verbal messages that might be left on answering machines or voicemail and also to information which is sent or received by email, fax, text or multimedia messages sent by mobile phone or other messaging services.

All media needs to be labelled with its classification category and managed as an asset.

10 Disposal of Information

Information which is no longer required must be disposed of safely and securely and in accordance with its protective marking. There are many reasons why care must be taken when personal information is to be disposed as follows:

- It could cause irreparable damage to individuals and families.
- It may cause damage to the Council's reputation if the information fell into the wrong hands;
- It would be a breach of the Data Protection Act.
- It could result in costly litigation and financial loss to the Council.

The ways in which we can prevent the above scenarios from occurring include the following disposal methods:

- To ensure that all information other than PUBLIC is securely shredded.
- Any media (tapes, USB memory sticks etc.) must be securely destroyed through the Council's disposal procedure.
- Records must be maintained of all media disposals and must be made readily available.

11 Copying Information

Employees should be aware that they should not copy by any means, information which is marked 'CONTROLLED' or 'RESTRICTED' unless they are authorised to do so, under the 'need-to-know' principle and all copies must be returned if the employee leaves the council.

12 Breaches Of Policy

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, agency staff, 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 contractor's non-compliance will result in the immediate removal of access to the system. If damage or compromise of the Council's ICT systems or network result from the non-compliance, the Council may 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, 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.