DERBYSHIRE County Council

Information Security Document

Information Classification and Handling Procedures

Version 9.0

Version History			
Version	**Date**	**Detail**	**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. Encryption Policy name update.	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			Jo White

This document has been prepared using the following ISO27001:2013 standard controls as reference:	
ISO Control	**Description**
A.8.2.1	Classification of information
A.8.2.2	Labelling of Information

1 Introduction

Derbyshire County Council is committed to the protection of all information and data regardless of the form it takes. Ensuring a consistent approach to the management and protection of information and data requires an information labelling and handling methodology and procedure. Access must be controlled and procedures which describe the level of protection required must be clearly defined.

The purpose of this procedure is to describe the methods of appropriate information classification and handling which applies to information both in electronic and physical forms.

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.

2 Procedure

The following procedures cover how to label, store, dispose of, communicate, physically transfer or copy different types of information, depending on its classification and media (e.g. paper, electronic transmission (email) or electronic storage/transfer).

The distribution of data should be kept to a minimum. However when data is required to be distributed it is required to be validated and have appropriate marking:

- To the authorised recipient (a formal record shall be maintained and reviewed at appropriate intervals by the authorised recipients of data); and

- Commensurate to its classification. That classification of data is split in to three categories as defined in the Information Classification and Handling Policy.

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

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

The agreed classification categories are:

- **PUBLIC**
  This is information that is freely available to anyone, e.g. information that is provided in flyers, leaflets, press releases, or on the Council website and does not require any access restrictions

- **CONTROLLED**
  This information is generally available to anyone within areas of the Council and contains business value to the organisation or requires protection due to personal data

- **RESTRICTED**
  Access to this information must be restricted to personnel with specific roles and clearance. Unauthorised disclosure of this information (even within the organisation) would cause serious damage in terms of financial loss, legal action, loss of reputation, damage to individuals and/or compliance with the GDPR.

LABELLING

Document authors will need to ensure that classification status markings are applied manually to all documents using the appropriate classifications of '**PUBLIC**', '**CONTROLLED**' or '**RESTRICTED**'.

All data must be marked with the appropriate classification clearly 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.

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 a document, particularly if consideration is being given as to whether a document should be disclosed, MUST consider the content of the document in determining how that document should be processed and not rely on its classification under this policy. The labelling of a document as controlled, restricted or public does not override the Council's duties under the Data Protection Act or the Freedom of Information Act 2000.

Classification markings may be appended in order to provide for more descriptive handling e.g:

PUBLIC – ISMS DOCUMENT
CONTROLLED – PERSONNEL RECORDS
RESTRICTED – ADOPTION RECORDS, BUSINESS CONTINUITY PLANS

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.

STORAGE

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

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

- CONTROLLED data:
  If information is removed from the Council for use by home workers it must not be left unsecured in employee's vehicles 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 data:
  This information is sensitive information of which access must be restricted - 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, data must be protected by the use of both technical and physical access controls.
The following must be in place for:

Restricted Data stored on servers:

- Servers must be located within secure rooms at Derbyshire County Council premises and 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 Data 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 possiblilty of ‘Shoulder Surfing’ or casual viewing by unauthorised people
- Data must be moved from the laptop to a secure area on the Council network as soon as possible

Restricted Data 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 Derbyshire County Council employee’s 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 employee’s vehicles or left in public places.
- Data 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 an other 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.

TRANSMISSION OF INFORMATION

The following table illustrates the information classifications that can be transmitted via the various transmission methods available to the Council:

Transmission Method	**PUBLIC**	**CONTROLLED**	**RESTRICTED**
By internal mail within the same building	☑	☑	☑
By internal mail between sites	☑	☑	☑
By standard post to UK/EU destinations*	☑	☑	☑
By recorded/special delivery to UK/EU destinations[1]	☑	☑	☑
By courier to UK/EU destinations	☑	☑	☑
By facsimile to UK/EU destinations[1]	☑	☑	☑
By encrypted email internal to the Council**	☑	☑	☑
By unencrypted email external to Derbyshire County Council to UK/EU destinations	☑	☑	☒

By encrypted email external to Derbyshire County Council to UK/EU destinations	☑	☑	☑
Across secure transmission link i.e. VPN	☑	☑	☑
By encrypted media (e.g. encrypted data sticks)	☑	☑	☑
Telephone & Video Conferences	✓	✓ provided the caller has been identified and is entitled to receive the information and the call is not in a public area.	✓ 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	✓	X	X

* consideration should be given to whether special or recorded delivery is required.
** Derbyshire County Council email is encrypted (internally) in transit. Delegates to mailboxes must be deemed to have the same access rights to the information held in the email as the mailbox owner.

All Derbyshire County Council emails will be classed as **‘CONTROLLED’.** The status may be changed to **‘PUBLIC’** or **‘RESTRICTED’** as required.

Whenever data classified higher than ‘**PUBLIC**’ is to be transmitted to a destination **outside** of the European Union (EU), advice must be sought from the ICT Service.

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, protect 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.

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 sensitive information is to be disposed as follows:

- 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 2018 and the GDPR.
- It could result in costly litigation and financial loss to the Council.
- It could cause irreparable damage to individuals and families.

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

COPYING

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.

This procedure applies to all information and documents produced by the Council which have been deemed to have a security classification applied to them. The information covered in this procedure 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).

All council information has a value to the organisation, however not all of the information has an equal value or required the same level of protection. Being able to identify the value of information assets is key to understanding the level of security that they require. Once the appropriate level of security is identified the appropriate control can be implemented to prevent loss, damage of 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 might result in inadequate or incorrect controls being implemented to protect them.

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.