Information Security Document

Information Classification and Handling Policy

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. 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.	Jo White

This document has been prepared using the following ISO27001:2013 standard controls as reference:	
ISO Control	**Description**
A.8.2.1	Classification guidelines
A.8.2.2	Information labelling and handling
A.18.1.3	Protection of Organisational Records

1 Introduction

Derbyshire County Council is committed to the secure management of its information and the identification of assets that require protection. For the purpose of this policy an asset is defined as functions, equipment and information that are deemed to have value to the organisation.

2 Purpose

The purpose of this policy is to establish the key principles of appropriate information classification and handling which applies to information both in electronic and physical forms.

3 Scope

The scope of this policy extends to all information and documents produced by the Council 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).

4 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 security that they require. Once the appropriate level of security 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.

4.1 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.

Classification	Description	Restrictions	Examples
Restricted	Information whose unauthorised disclosure (even within the organisation) would cause serious damage in terms of financial loss, legal action, loss of reputation, damage to individuals and/or	Access is restricted to personnel with specific roles and clearance or with statutory rights of access	• Adoption records. • Child Protection records. • Disciplinary records. • Social Care files with local restrictions eg family members. • Court Proceedings.

	compliance with the GDPR.		• Public Health data containing PCD. • 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 DCC 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	• 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	None	• 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. • Trading Standards Judgements.

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

All information must be categorised using either '**PUBLIC**', '**CONTROLLED**' or '**RESTRICTED**' and must be appropriately labelled. 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, the GDPR or the Freedom of Information Act 2000.

Once a document 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 a document 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 vital.

4.2 Information Handling

The following table provides electronic information handling guidance for classifications described in section 4.1. All hardcopy information needs to be stored and handled as specified in the Information Classification and Handling Procedures. 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.

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

4.3 Information Transmission

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

Transmission Method	Public	Controlled	Restricted
By internal mail within the same building	✓	✓	✓
By internal mail between buildings	✓	✓	✓
By standard post to UK/EU Destinations*	✓	✓	✓
By recorded/special delivery to UK/EU destinations	✓	✓	✓
By courier to UK/EU destinations	✓	✓	✓
By facsimile to UK/EU destinations	✓	✓	✓
By encrypted email internal to the organisation**	✓	✓	✓
By unencrypted email external to Derbyshire County Council to UK/EU destinations	✓	✓	X

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 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 Union (EU), advice must be sought from the ICT Service.

5 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, 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 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.