Corporate Records Management Policy

1. Version History

1.0 2007 Published Derbyshire Record Office

2.0 26/05/2011 Reviewed and approved by Information Governance Group. Revamped from original document. David Jenkins

3.0 30/05/2012 Reviewed by Information Governance Group. David Jenkins

4.0 27/06/2013 Reviewed by Information Governance Group. David Jenkins

5.0 14/07/2014 Reviewed by Information Governance Group. David Jenkins

6.0 12/10/2015 Reviewed by Information Governance Group. David Jenkins

7.0 07/11/2016 Reviewed by Information Governance Group. David Jenkins.

8.0 04/12/2017 Reviewed by Information Governance Group. No changes. Mark Smith

9.0 16/02/2018 Addition of role descriptions for Information Risk Owners and Data Protection Officer, as requested by Information Commissioner's Office. Other minor changes to wording. Mark Smith

10.0 07/05/2019 Reviewed by Information Governance Group. No changes. Mark Smith

11.0 16/06/2020 Reviewed by Information Governance Group. No changes. Mark Smith

12.0 06/07/2021 Reviewed by Information Governance Group. No changes. Mark Smith

13.0 02/08/2022 Revisions drawing on suggestions from Audit Services. Introduction notes benefits of openness, scope aligned with Information Asset Management Policy, objectives refreshed, key concepts expanded, Appendix A replaced by cross-reference to applicable legislation register, Appendix B re-labelled. Mark Smith / Philip Spencer

14.0 06/09/2023 Reviewed by Information Governance Group. Agency staff added. Mark Smith

15.0 08/10/2024 Reviewed by Information Governance Group. ISO27001 controls updated. Mark Smith

16.0 11/11/2025 Reviewed by Information Governance Group. Business classification scheme and specification for record keeping system requirements added. Mark Smith

17.0 10/03/2026 Reviewed by Information Governance Group. Incorporated Information Classification and Handling Policy, Document and Record Control Procedures and Record Disposal Policy and Procedures. Mark Smith

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.5.12-13-Classification and Labelling of Information

A.5.31-Legal, statutory, regulatory and contractual requirements

A.5.33-Protection of records

A.5.34-Privacy and protection of PII

A.6.3-Information security awareness, education and training
A.7.10-Storage Media

2 Introduction

This policy sets out a framework for comprehensive records management arrangements, as required by the Code of Practice issued under Section 46 of the Freedom of Information Act 2000 ("the Records Management Code"). The Records Management Code requires every public authority to identify its own information needs, and to manage its records in accordance with them.

For Derbyshire County Council, information and records are essential. The Council depends on them to conduct its business, comply with legislation, and demonstrate accountability.

Information is valuable. It must therefore be carefully protected and made available only to individuals with a legitimate need of access. However, not all information has equal value or requires the same level of protection. When an appropriate level of protection is identified, security classification helps prevent data from being lost, damaged, compromised or stolen. This policy defines the Council's security classification system. Compliance with it lowers the risk of harm to the council and the people it serves.

Records are among the Council's most important assets. They form the corporate memory of Council policies, services and decision-making processes. Compliance with this policy will help the Council produce reliable evidence, defend itself from legal claims, and act with transparency. According to research undertaken for the Organisation for Economic Co-operation and Development (OECD), greater openness incentivises better records management to the benefit of citizen and government alike, making decisions and services more efficient and serving as a safeguard against misgovernment and corruption.

3 Policy Statement

The Council is committed to managing its information securely and efficiently. This begins before the information is even created, as systems are designed and configured. Information needs active management throughout its lifecycle, from classification and storage to secure disposal. The Council will make effective use of its records to deliver public services, document its principal activities and maintain the corporate memory. Records management principles will be embedded in the Information Security Management System to support the authenticity, reliability, integrity and usability of the Council's records. Continuous review of the policies, procedures and guidance contained in the system will be informed by ISO 15489 (the international standard on records management), the Records Management Code and examples of best practice.

4 Scope

The scope of this policy extends to all Council departments, employees, agency staff, elected members, third parties, vendors and partner agencies who use Council information and records. This data may be held in hard copy or electronic format, shared verbally or visually (e.g. via telephone conversations or Teams calls).

5 Objectives

The objectives of this policy are to ensure that the Council

- creates documents that are properly titled, referenced and indexed
- applies security classification markers to its information
- arranges records according to a Business Classification Scheme

- keeps information secure while allowing timely retrieval, supporting resilience
- reduces risk of regulatory intervention and legal claims
- complies with legal and regulatory requirements, including those listed in the applicable legislation register
- keeps records for as long as is necessary to meet its business needs and all legal, administrative and financial requirements
- disposes of time-expired records promptly, to minimise costs and manage storage space efficiently

6 Key Concepts

6.1 Information

Information is data that is organised and contextualised so it can be understood.

6.2 Documents

A document is a self-contained unit of information. It may be understood on its own or through use of other information sources. Practices which govern the proper management of documents may apply equally well to any data. For instance, a row in a relational database table may be regarded as a manageable unit, relating to a single transaction which can be understood independently.

6.3 Records

Records are defined as “Information created, received, and maintained as evidence and as an asset by an organisation or person, in pursuit of legal obligations or in the transaction of business” (ISO 15489-1). A recordkeeping system may be defined as any system which maintains the authenticity, reliability, integrity and usability of such information. Where signatures are used to authenticate records, an electronic signature applied through an auditable system is as valid as a wet signature, provided appropriate identity and access controls are in place.

The Records Management Code leaves it to each authority to decide on the value of its information and the purpose of holding it. The Council acknowledges its responsibility to manage its information assets, especially those containing personal data (see the Corporate Data Protection Policy and the Information Asset Management Policy) and to maintain the evidential value of those assets which it regards as records.

This definition of “records” excludes information with no evidential value, i.e. transient data. Transient data may be held within electronic systems with continuous data flows, or could be in hard copy, like a page torn from a notepad. Transient data is of short-term transactional value only. For instance, Council staff may use a diary as an aide memoire to facilitate capture of information in a recordkeeping system, but this does not make the diary a record. Transient data must nevertheless be managed securely as it may include sensitive, personal or confidential information.

6.4 The information lifecycle

Information moves through several defined phases:

- **Creation:** Information is generated or received in support of business functions, defined in the Council’s Business Classification Scheme. It is protected in accordance with its security classification.
- **Capture:** Information meeting the definition of Records must be stored in a repository which meets the Council’s system requirements.
- **Current:** Current Records are evidence of Council business and are in frequent use. They may take the form of active client files, active correspondence (paper and email), reports etc.

- **Semi-Current:** Semi Current Records require continued retention but see less regular use. They include inactive client files, financial records, and records retained purely for compliance purposes.
- **Disposal:** Non-Current Records are no longer required either for the conduct of current business or for compliance reasons and should be disposed of.

7 Key Controls

7.1 Business classification

A Business Classification Scheme (BCS) is a conceptual representation of an organisation's business. The Council's BCS uses a conventional three-level structure to produce a unique reference. The levels are Function, Activity, Transaction. For example:

Function: Finance

Activity: Provision management

Transaction: Maintaining ledgers

Reference: FIN 01.01

The Council's BCS forms the framework for its retention schedules and an index to the Record Of Processing Activity. Using a consistent file naming convention and recording the BCS reference in metadata makes information easier to discover as a current or semi-current record and easier to dispose of at the end of the lifecycle.

7.2 Security classification

All information must be categorised as Restricted, Controlled or Public and must be labelled accordingly:

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 to compliance with the UK General Data Protection Regulation (UK GDPR). Access is restricted to personnel with specific roles or access rights. It must be kept in secure conditions. Home-workers must take extra care with Restricted information to avoid accidental disclosure to any unauthorised person, including family members. It should be stored in a lockable area when in the employee's home and should not be left unattended in a vehicle (including in the boot overnight). Employees should not copy Restricted information without authorisation and must return or destroy copies before leaving the Council.

Examples:

- Adoption records.
- Child Protection records.
- Disciplinary records.
- Social Care files with local restrictions e.g., family members.
- Family/Youth Court Proceedings.
- Patient Confidential Data including occupational health
- Audit Reports.

Restricted information must be managed subject to the access controls described in Appendix E.

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 council staff in connection with their

employment. It must be kept in secure conditions. As with Restricted information, home-workers must take steps to avoid accidental disclosure of Controlled information and must return or destroy any copies before leaving the Council.

Examples:

- Social Care information not in Restricted.
- IT Procedures relating to the Data Centres, Network, Backups etc.
- Personnel files.
- Contracts.
- Council exempt papers unless with a restricted section.
- Commercially sensitive files.
- Draft service 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.
- Minutes other than exempt.
- Statistics & Performance Indicators.
- General recruitment information and terms of conditions of employment.

Mixed classifications

Where information is grouped together, the highest classification must be applied to all information in the group. Information of any classification should be managed in accordance with the handling guidance in Appendix C and transmission guidance in Appendix D.

Security classification may change over time. For instance, a document may have a 'Restricted' classification early in its lifecycle, downgraded to 'Controlled' as time progresses. The same record might then become 'Public' if transferred to Derbyshire Record Office for permanent preservation.

7.3 Record keeping systems

For information to be maintained as a record, it must be captured in a recordkeeping system. Digital Services will maintain a specification defining minimum requirements for electronic recordkeeping systems, including metadata capture, version control and digital preservation. This specification should be kept under regular review. It should be flexible enough to balance demands for functionality and affordability, without sacrificing security.

It follows that information should not generally be stored locally on individual devices. Where a dedicated case management system (e.g. Mosaic) has been adopted, it should be used to capture all appropriate information. The Council's corporate electronic document and records management system (EDRM) is suitable for most other Council records. Where neither a case management system nor the EDRM is in use, a shared network drive with appropriate access controls should be used.

Although the Council is committed to working digitally wherever possible, consideration should be given to the proper storage of paper records. Storage arrangements should reflect the business value and security classification of the information in question. Storage conditions must protect records from damage or deterioration (e.g. in damp conditions) and from unauthorised access.

7.4 The Record Of Processing Activity (ROPA)

A ROPA is a high-level description of how and why a data controller uses personal data. Article 30 of UK GDPR and Section 61 of the Data Protection Act 2018 require the Council to maintain its ROPA to show to the Information Commission on request. The Corporate Records Manager is responsible for co-ordinating the regular review of ROPA with the relevant Information Asset Owners (IAOs). IAOs remain responsible for the accuracy and quality of the content, subject to the Information Asset Management Policy. The interval between reviews should not exceed two years. Minor changes may be made to ROPA entries at any time, without waiting for formal review, in consultation with the Corporate Records Manager. For details, see the ROPA Procedures.

7.5 Retention schedules

Records must be disposed of at the end of their lifecycle, to facilitate efficient access to information and economical use of storage (physical and electronic). This is especially important with records containing personal data, as UK GDPR requires it to be kept for no longer than necessary for the purpose of processing. However, disposal does not always mean destruction: UK GDPR also allows "archiving purposes in the public interest", to support scientific, historical or statistical research. Records of potential historical value should therefore be offered to Derbyshire Record Office.

Disposal decisions must be guided by the Council's retention schedules. A retention schedule is a document which determines the appropriate retention periods for records, drawing on compliance requirements, common practice and business need. Rules in the Council's retention schedules use a limited range of time periods, defined in the Standard Operating Procedures.

The Corporate Records Manager is responsible for co-ordinating the regular review of retention schedules with the relevant Information Asset Owners (IAOs). IAOs remain responsible for the accuracy and quality of the content. The interval between reviews should not exceed two years. As with ROPA, minor changes may be made at any time in consultation with the Corporate Records Manager.

7.6 Destruction Certificates and Archival Transfer

Disposal is the process which determines the final fate of a record. It can include destruction, transfer to another body, or permanent retention. To qualify for permanent retention, records must be:

- needed for as long as the Council is in existence
- required to satisfy a permanent legal requirement, or
- part of the Council's historical archives held at the Derbyshire Record Office

Approximately 10% of rules in the retention schedules recommend permanent preservation at the record office. Permanent records include minutes of the County Council, audited annual accounts and title deeds. Such records series may be suitable for storage by the Modern Records service during their semi-current phase.

The remaining 90% of rules require destruction on expiry of the retention period. Destruction means the data is made permanently unavailable, so that it cannot be recovered by any means reasonably likely to be used. Destruction should be authorised by two members of staff, typically someone with operational responsibility for the records and their line manager. This authorisation should be recorded using a destruction certificate, which captures evidence of disposal alongside a high-level summary of what was destroyed (e.g. case files of pupils aged 25 years or over as of 1st April 2022). For further details, see the Record Disposal Procedures and the Secure Destruction of Optical and Magnetic Media Procedures.

A certificate is not required for routine destruction of transient data such as backups. According to the Information Backup and Restore Policy, backups are routinely created to allow information to be restored in the event of loss, corruption, damage or unavailability. The timing of regular destruction must therefore meet this business need, without reference to the disposal criteria applicable to the original content.

Similarly, a destruction certificate is not required when records are scanned from paper originals and stored in a suitable recordkeeping system. Provided digitisation is carried out according to the Corporate Scanning Policy, the record continues to exist in a new format, following destruction of the hard copy.

8 Responsibilities

8.1 Caldicott Guardian:

The role of Caldicott Guardian originated in the National Health Service after the 1997 publication of Dame Fiona Caldicott's report into the handling of patient-information, before being introduced into local authority social care in 2002. Derbyshire County Council's Caldicott Guardian is responsible for:

- acting as the conscience of the organisation, ensuring that legal and ethical considerations are taken into account in the sharing of confidential information.
- promoting appropriate organisational culture, to encourage excellence in information governance
- arbitrating in cases of disagreement about processes impacting on confidentiality

8.2 Information Risk/Asset Owners:

The Information Governance Group (IGG) co-ordinates the management of information assets through Information Risk Owners (IROs) and their appointed information asset owners (IAOs). The IGG is chaired by the lead officer on delivering risk management and security strategy in the Council, who is designated the Senior Information Risk Owner (SIRO). The SIRO is responsible for:

- overseeing the information security and governance function
- overseeing incident management and risk management
- overseeing security management and reporting, including maintenance of the ISO27001 standard

Other IROs and IAOs are responsible for:

- the routine management, review and treatment of risks to the Council's information assets
- undertaking quarterly reviews of information risk assessments, in line with the requirements set out in ISO27001
- participating in review of retention schedules and ROPA alongside the Corporate Records Manager, or delegating this role

For more information, see the Information Asset Management Policy.

8.3 Elected Members

Elected Members are responsible for ensuring that:

- records management is recognised as a mandatory corporate function within Derbyshire County Council
- records management receives the necessary levels of organisational support and resources required to ensure effectiveness

8.4 Department/Service/Section Heads

Department/Service/Section Heads are responsible for ensuring that:

- agreed Corporate Records Management policies, procedures and retention schedules are implemented and adhered to within their areas
- appropriate staff are designated to assist with the implementation of records management policies and procedures and liaise with the Corporate Records Manager
- staff are given training to carry out records management duties, as well as sufficient time and resources for a large-scale record disposal such as may accompany an office relocation
- they promote regular disposal of records and provide authorisation for destruction or transfer to Derbyshire Record Office

8.5 Data Protection Officer

The Council appoints a Data Protection Officer (DPO) in accordance with the requirements of the UK General Data Protection Regulation (GDPR). The DPO is accountable to the Council via the Corporate Management Team to:

- inform and advise the organisation and its employees about their obligations to comply with the UK GDPR and other data protection laws
- monitor compliance with the UK GDPR and other data protection laws
- be the first point of contact for supervisory authorities and for individuals whose data is processed.

8.6 Archives and Local Studies Manager

The Archives and Local Studies Manager is responsible for ensuring that

- appropriate advice and guidance is given to Elected Members and Senior Officers to establish and maintain a corporate framework for the management and preservation of records in all formats across the Council
- professional standards for records management, archive management and preservation are met and compliance with records management policies and procedures are regularly reviewed
- records management strategies are developed, evaluated and revised, and advice on standards is provided
- the Corporate Records Manager is supported in their work in terms of supervision, learning and development and resources
- records identified for permanent preservation are transferred as appropriate to the Derbyshire Record Office
- Derbyshire Record Office continues to preserve and manage the historic records of Derbyshire County Council, and meets relevant national and international standards (BS4971:2017, ISO 15489 and Archive Service Accreditation)

8.7 Corporate Records Manager

The Corporate Records Manager is responsible for ensuring that:

- an effective and efficient records management programme is developed and implemented to enable the Council to meet its record keeping obligations
- sufficient advice and guidance is given to officers with records management responsibilities (see Records Management on Our Derbyshire)
- support and guidance is given towards the implementation and development to appropriate standards of a corporate EDRM
- records management guidance notes and procedures are developed and disseminated
- staff are trained in records management best practice and how to implement corporate records management policies and procedures
- the off-site document storage contract is coordinated effectively including the regular review of the operation of the contract

- the implementation of records management policies and procedures is monitored, evaluated and reported
- ROPA and retention schedules are arranged according to the Business Classification Scheme and are reviewed with Information Asset Owners or their delegates, within a maximum review window of 2 years

8.8 Individual Employees

Individual Employees are responsible for ensuring that:

- Council business activities and decisions are properly documented and recorded
- The Corporate Records Management policy is followed consistently with the support of the Corporate Records Manager
- Records are identified for disposal in accordance with agreed policies and retention schedules
- Disposal procedures are implemented consistently

9 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 parties in the scope of this policy have a responsibility to report security incidents as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation given access to Council information.

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.

10 Policy Monitoring and Review

Compliance with this policy and related standards and guidance will be monitored by the Corporate Records Manager and the Archives and Local Studies Manager in consultation with the Information Implementation Group.

A review of this policy will take place at least every two years to take account of any new or changed legislation, regulations or business practices.

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.

Appendix A: Partnership working

Derbyshire County Council carries provides services in conjunction with partner organisations, subject to the Information Sharing Policy. Derbyshire County Council has a responsibility to ensure records of partnership initiatives are properly managed.

This guidance is intended to eliminate duplication of records across stakeholders while preserving operational efficiency. Information sharing amongst partners and stakeholders is a key issue for effective delivery of services. Appropriate procedures for record creation and management must be developed which demonstrate compliance with central government advice, as well as with local policies and priorities.

Core records which need to be kept permanently should be identified and one partner made responsible for management and long-term preservation.

General Principles

Where Derbyshire County Council is the lead partner:

- The core records will be retained and managed by the Council.
- Retention rules will derive from the Council's retention schedules unless an alternative is agreed by all parties.
- The Council's Corporate Records Management policy will apply.

Where another organisation is the lead partner:

- The core records will be retained by the lead organisation.
- Derbyshire County Council should identify and manage the records relating to its role in the partnership. Many of these records will be operational and will therefore only need to be kept for a time-limited period.

Where no single organisation is the lead partner:

- Derbyshire County Council should ensure that provisions are made for one partner, whether this is the Council or another partner, to be responsible for management of the core records.
- If Derbyshire County Council is nominated to manage the partnership's records, then the Council's Corporate Records Management policy and procedures will apply.
- Derbyshire County Council should recommend to partners that an appropriate file plan is put in place and that consistent metadata standards, version control and file titling procedures are implemented to ensure that the records can be managed effectively and to agreed standards across the partnership.

Appendix B: Standard Operating Procedures for retention schedules

Introduction

Some documents do not need to be kept at all. Standard Operating Procedures (SOP) relate to items which you should routinely destroy in the normal course of business. This usually means material that is:

- Duplicated (e.g. copies of records securely held elsewhere, reports/minutes circulated among a team for short-term information, copies of official literature)
- Unimportant (e.g. trivial email messages or paper notes unrelated to council business, compliments slips and stationery)
- Of short-term transactional value (e.g. draft versions of a record, telephone messages slips after the message has been passed on)

There is no need to keep diaries or notebooks if the information has been transferred into a case management system.

Take time to make a conscious, positive decision about whether to keep or destroy documents. Make an exception for any document that you clearly need as key evidence, e.g. to prove that something happened or that a decision was reached, and capture it in a proper recordkeeping system. Where integrated records are managed in an electronic case management system, they should only be destroyed when all applicable retention periods have expired. This means system user data such as an employee's name and job title may be retained within case records, beyond the retention period of their personnel file.

Never destroy information which is the subject of an ongoing Subject Access Request, Freedom of Information request, legal claim, audit investigation or similar official enquiry. This may be a criminal offence under UK law.

If in doubt, contact the Corporate Records Manager.

Glossary

- Business need / Common Practice: if no law or regulation to says how long a record should be kept, we consider our administrative needs, or what similar organisations do
- Closure: when a record ceases to be 'current' – e.g. a set of minutes is formally agreed
- Disposal: processes associated with the end of a record's lifecycle, including destruction, or transfer to Derbyshire Record Office
- Offsite Storage: you may only use Derbyshire County Council's preferred provider. Contact your line manager or the Corporate Records Manager to discuss this option.
- Permanent: Retain the record permanently and offer to Derbyshire Record Office
- Record: information kept as evidence of an activity
- Disposition: what to do with the record, triggered by a particular event (e.g. its closure)

The 6 Plus Rule and other standard retention periods

For simplicity, Derbyshire County Council has a default rule for records, known as the 6+ Rule. It means: destroy six years from the end of the financial year in which the record was last modified. This aligns with the right to launch certain types of claim under the Limitation Act 1980. In systems which use calendar rather than financial years, retention should be rounded up to 7 years.

Where the 6 Plus Rule is not appropriate, other standard retention periods are available:

- DOB+25: Destroy 25 years after date of birth – useful for records relating to minors, who may possibly launch a legal claim on reaching maturity.
- DOB+35: Destroy 35 years after date of birth
- DOB+100: Destroy 100 years after birth – approximately, lifelong retention
- CASE+25: Destroy 25 years after entire case is closed
- CASE+6: Destroy 6 years after entire case is closed
- ACTION+15: Destroy 15 years after last action, use or modification.
- ACTION+25: Destroy 25 years after last action, use or modification.
- ACTION+50: Destroy 50 years after last action, use or modification.
- ACTION+75: Destroy 75 years after last action, use or modification.
- ACTION+100: Destroy 75 years after last action, use or modification.
- TERMS+6: Destroy 6 years after expiry of terms of e.g. ordinary contract.
- TERMS+12: Destroy 12 years after expiry of e.g. sealed contract.
- D<1: Destroy within one year, e.g. transient data awaiting final deletion.
- PERM: Offer to Derbyshire Record Office when no longer required. Before transferring any records, you must complete a deposit request form.

The above disposition codes are used throughout the retention schedules.

Where none of these options is acceptable, the Corporate Records Manager and retention schedule owner can agree on an addition to the list above, which is appended to the record disposal policy to allow for regular review by Information Governance Group.

Examples of transient data

In the retention schedules, the disposition code D<1 refers to transient data. The Management & Administration of Records retention schedule defines transient data as “data in transit to a council-approved recordkeeping system, or transit to final deletion” and requires destruction after transit.

Completion of transit may mean:

- closure of hard copy transient record (e.g. notebook, signing-in sheet)
- transfer of information/file into a case management system
- transfer of file into electronic document/record management system
- transfer of file into shared network drive
- alteration of a web page
- final removal of a web page
- expiry of an automated waiting period imposed for disaster recovery, business continuity or data security reasons.

In the interests of information security, disaster recovery and business continuity, a short waiting period of up to one year may be observed before deletion of transient data. Some examples:

- 2-week rolling destruction programme on datasets shared by external agencies in the interests of Community Safety. Subjects include: modern slavery, child sexual exploitation, organised crime, prevention of terrorism.
- 30-day rolling destruction programme on telephone call recordings handled in a contact centre (telephone recordings may also be retained for training and quality control purposes - see Contact Centre retention schedule).
- 30-day rolling destruction programme on audio recordings of meetings produced to allow for verbatim transcription.

- 60 day rolling deletion of web content not modified within previous 12 months
- 30-day rolling destruction of deleted web content in the Contents Management System
- 4-month destruction on domestic abuse notifications made to Children's Services.
- 90-day rolling destruction programme on backups of the Library Management System
- 6-month rolling destruction programme on operational data and system backups used in maintenance of other ICT infrastructure.
- 6-month rolling destruction programme on user-deleted documents in the Electronic Document and Records Management system.
- 6-month rolling destruction programme on the personal workspaces of former employees, temporarily held in the Electronic Document and Records Management system for review by line managers.
- 1 year manual destruction of working documents to do with emergency planning, after their transfer to a final record.
- 1-month retention of non-DCC user accounts in the learning and development system, starting with notification that the account is inactive
- 2-month rolling destruction of interface files used in personnel recordkeeping, where the source and target systems hold a full record in accordance with the HR retention schedule
- 2-month rolling destruction of interface files used in financial recordkeeping (excluding Adult Care and Fostering), where the source and target systems hold a full record in accordance with the Finance retention schedule

Appendix C: Information Handling guidance table

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

Appendix D: Information Transmission guidance table

The following table provides guidelines on methods of information transmission.

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.

Appendix E: Access Controls for Restricted Information

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 removable media, such as 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
- 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.

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