DERBYSHIRE
County Council

Information Backup and Restore Policy

1 Version History details and author

1.0	25/03/2011	Completed for distribution	Jo White
1.0	31/03/2011	Approved by Information Governance Group	Jo White
2.0	25/04/2012	Reviewed by Information Governance Group	Jo White
3.0	31/05/2013	Reviewed by Information Governance Group	Jo White
4.0	16/06/2014	Reviewed by Information Governance Group	Jo White
5.0	13/07/2015	Reviewed by Information Governance Group	Jo White
6.0	09/08/2016	Reviewed by Information Governance Group	Jo White
7.0	09/10/2017	Reviewed by Information Governance Group. Transformation changed to ICT. Amendment to restores over 30 days.	Jo White
8.0	05/11/2018	Reviewed by Information Governance Group. No changes.	Jo White
9.0	18/12/2019	Reviewed by Information Governance Group. Server Team changed to Data Centre Team.	Jo White
10.0	12/01/2021	Reviewed by Information Governance Group. No changes.	Jo White
11.0	08/02/2022	Reviewed by Information Governance Group. Requirement for recording mechanism removed. Data Centre replaced by Operations.	Jo White
12.0	07/03/2023	Reviewed by Information Governance Group. Storage of data on mobiles removed.	Jo White
13.0	14/05/2024	Approved by Information Governance Group. ISO27001 controls updated. Photocopies removed. ICT changed to Digital.	Jo White

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

A.5.3 - Segregation of duties
A.5.12 - Classification of information
A.7.10 - Management of removable media
A.7.10 - Disposal of media
A.7.10 - Physical media transfer
A.7.1 > 6 - Secure areas
A.7.14 - Secure disposal or re-use of equipment
A.5.37 - Documented operating procedures
A.8.13 - Information backup

2 Introduction

Derbyshire County Council has a duty to ensure that all information and data which it is responsible for is securely and routinely backed up. The Council has a responsibility to ensure that information and data which has been backed up can be restored in the event of deletion, loss, corruption, damage or made unavailable due to unforeseen circumstances.

3 Purpose

The purpose of this policy is to identify and establish processes, procedures and good working practices for the backup and timely recovery of the Council's information and data existing in both electronic and physical form.

4 Scope

The scope of this policy extends to the back-up of all important information and data regardless of the form it takes - including the recovery of IT systems and supporting infrastructure.

5 Policy Statement

There is always a risk that systems and/or procedures will fail resulting in loss of access to information, data and systems, despite the implementation of best practice. The following steps will help ensure the Council's information and data is backed up and restored securely in the most efficient manner possible:

IT SYSTEMS/DATA BACKUPS

1. The Council's IT administrators are responsible for providing system support and data backup tasks and must ensure that adequate backup and system recovery practices, processes and procedures are followed in line with the Council's Disaster Recovery Procedures and departmental data retention policies
2. All IT backup and recovery procedures must be documented, regularly reviewed and made available to trained personnel who are responsible for performing data and IT system backup and recovery
3. All data, operating systems/domain infrastructure state data and supporting system configuration files must be systematically backed up - including patches, fixes and updates which may be required in the event of system re-installation and/or configuration
4. Wherever practicable, backup media (e.g. tape) must be encrypted and appropriately labeled. Any system used to manage backed-up media should enable storage of date/s and codes/markings which enables easy identification of the original source of the data and type of backup used on the media. All encryption keys should be kept securely at all times with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster
5. Copies of backup media must be removed from devices as soon as possible when a backup or restore has been completed
6. Backup media which is retained on-site prior to being sent for storage at a remote location must be stored securely in a locked safe and at a sufficient distance away from the original data to ensure both the original and backup copies are not compromised by the same event.
7. Access to the on-site backup location and storage safe must be restricted to authorised personnel only

8. All backups identified for long term storage must be stored at a remote secure location with appropriate environmental control and protection to ensure the integrity of all backup media
9. Backup media must be protected in accordance with the Council's Physical and Environmental and Data Protection and Media Handling Policies
10. Hard copy paper files containing important information and data should be scanned and stored electronically to ensure digital copies are created which can be backed up by the Council's ICT systems. Where this may not be possible, additional security measures must be considered.
11. Regular tests must be carried out to establish the effectiveness of the Council's backup and restore procedures by restoring data/software from backup copies and analysing the results. Departmental IT Service Relationship managers should be provided with information relating to any issues with the backup testing of their data
12. The Digital Services Operations team should maintain a record of job failures, with the re-running of any failed jobs logged in the backup software management console.
13. Backup data/media no longer required must be clearly marked and recorded for secure disposal and with due environmental consideration (subject to the Waste Electrical and Electronic Equipment Regulations 2013) – more information is available at: staff.derbyshire.gov.uk/disposing

USER RESPONSIBILITIES

IT Users also have a responsibility to ensure Council data is securely maintained and is available for backup:

1. IT Users must not store any data/files on the local drive of a computer (this excludes the normal functioning of the Windows operating system and other authorised software which require the 'caching' of files locally in order to function). Instead, Users must save data (files) on their allocated areas – this could be an area within the EDRM system, a mapped drive or network shared folder the User has access to. Data (files) which are stored "locally" will NOT be backed up and will therefore be at risk of exposure, damage, corruption or loss.
2. If the Council network becomes unavailable for whatever reason and work related data is at risk of being lost, users have no option but to save the data (files) locally (i.e. on the computer being used) or on approved media storage such as a Council owned encrypted Data stick (USB storage). Once the Corporate Network becomes available again, data (files) should be immediately transferred to the Corporate network in order for it to be backed up safely and local copies of data on the computer or portable storage media should be deleted. This will help to ensure the availability and integrity of data and to avoid duplicate copies of data being stored
3. Only Council purchased and encrypted USB data sticks should be used and any data stored must be for temporary purposes. All sensitive, business and personal identifiable information should be removed from the USB data stick and moved to an appropriate Council data network location as soon as possible in order to ensure the data is made available to the Council and can be successfully backed up

DATA RESTORES

The Council has well established backup and restore routines in place. Data (file) restores are normally carried out by the Operations team who will endeavour to restore files from a date specified by the user or from the nearest backed up date

1. IT Users must request data (files) to be restored by contacting the Digital Services Service Desk, preferably by raising a call using the HALO ITSM online facility. Only files which the user is authorised to access will be provided from the restore
2. The Operations team will need to verify that the User has permission and/or authorisation to view or obtain restored copies of file/s and/or folder/s.
3. Restores requested for information older than 30 days will need to have further departmental approval before being undertaken. Backups are kept for a maximum of six months after which no restores will be possible.
4. Content will be restored to the same source folder or the same area, so any requestor will need access to that folder/area to access the restored file.
5. Users requesting a restore/s are required to provide as much information about the data (file/s) as necessary – this will include:

    - The reason for the restore
    - The name of file/s and/or folder/s to be restored
    - Original location of file/s and/or folder/s - the Service Desk will provide guidance to the User on how to find this out
    - Date, day or time of deletion/corruption or nearest approximation
    - The last date, day or time which the User recalls the data (files) being intact and accessed/used successfully

6. All backup and recovery (restore) procedures must be documented and made available to Data Centre personnel responsible for carrying out data (file) restores
7. Requests from third party software/hardware vendors for file or system restores for the purpose of system support, maintenance, testing or other unforeseen circumstance should be made under the supervision of the Operations team via the Council's Digital Services Service Desk
8. Personnel accessing backup media for the purpose of a restore must ensure that any media used is returned to a secure location when no longer required (applies to media from both Council and remote storage locations)
9. A log must be maintained to record the use of backup media whenever it has been requested and/or used from secure storage
10. If data is deleted in response to an individual rights request under the Data Protection Act 2018, it should be excluded from any subsequent restore, or deleted again immediately after a required restore is complete.

The Data Centre is a sensitive area and specific technical information regarding the detail of backup and restore procedures is held by the Head of Operations

6 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or 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 individual 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.