Corporate Ref.	FEIT 008
Level	3
Senior Responsible Officer	Chief Executive Officer
Version	2
EIA	N/A
Approved by	Chief Executive Officer
Approved date	3 June 2024
Superseded version	1
Review date	3 June 2025

Back-up and Archiving of Data Held on IT Systems Policy

Version Control

Version	Author	Date	Changes
2	Digital Infrastructure Service Lead	27/05/2024	Moved to new template and narrative updated.

1. INTRODUCTION

Effective data backup and archiving are critical components of the College's information security strategy, aimed at ensuring data security, business continuity, and disaster recovery.

This policy outlines the procedures and responsibilities for backing up and archiving data held on IT systems. The primary goal is to maintain the availability and integrity of data, ensuring it is accessible when needed by authorised personnel while protecting it from loss, corruption, or unauthorised access.

2. OBJECTIVES

The objective of this policy is to ensure the effective management and protection of the College's data through comprehensive backup and archiving strategies. This includes adhering to all relevant legal, regulatory, and compliance requirements concerning the backup and archiving of data, and aligning with data protection laws, industry standards, and College policies.

The policy aims to protect data from loss, corruption, and unauthorised access through measures such as isolation, encryption, and multi-factor authentication. Establishing reliable backup and archiving systems is essential for business continuity and disaster recovery efforts, allowing the College to quickly recover from data loss incidents, system failures, or other disruptions.

3. SCOPE

This policy applies to all data managed by the College’s digital information systems, encompassing a wide range of data types critical to the College’s operations. It includes data related to learning and teaching, administrative and management information, and centrally held user data. The policy covers both on-site and off-site storage solutions, ensuring comprehensive data protection across various storage environments.

This policy mandates that all College-related work be saved to College systems to ensure appropriate backups. This includes data stored on central administrative systems, academic servers, and infrastructure servers, as well as data held within cloud services.

This policy does not cover data that has not been saved to the College network or has been saved to removable devices owned by individuals or departments. Such data is excluded from the College's backup and archiving processes. Additionally, backup policies for third-party solutions, such as Office 365, are governed by specific agreements and may differ from those applied by the College's IT team.

4. CORE POLICY

The IT team centrally stores and backs up the key data and data sets upon which the College relies. Back-up procedures and archiving retention periods correspond to sector best practice, which overlay legal requirements. These procedures are also shaped by local requirements informed by the College's business objectives, those being, primarily, learning and teaching, and associated administrative/ operational requirements.

The College maintains backups of data, logging information, and applications and systems software held on central administrative, academic and infrastructure servers including 'cloud' services. Data are backed-up daily (or on occasions following every working day in the case of some administrative backups), with backups held separate from the original copies on disk on computers in separate data centres or through 'cloud' services. At least weekly in any case all data are backed up. Any back-up tapes used are kept in fire safes remote from the servers they back up.

The following retention details and backup strategies are applied:

- Primary storage - default retention must retain all backups for 14 days or a complete backup cycle, whichever is longer. Weekly backups must be retained for one month, and monthly backups retained for three months.

- To provide additional redundancy and security, a synchronous copy of the primary backups must be maintained at a second location, also retained for 14 days by default, retaining weekly backups for one month, and monthly backups for 3 months.
- Quarterly full backups are conducted and retained for 365 days, ensuring long-term data availability for critical recovery scenarios.
- A remote cloud copy of recent backups is stored with a default retention of 14 days and extended storage or weekly full backups, providing an off-site storage solution for enhanced data protection.

Backups are run overnight to minimise impact on service provision during the day. They are stored in two alternative campus locations and in secure locations with access limited to authorised personnel only. Requests for backup data from third parties must be approved by the Chief Operating Officer in consultation with the Data Protection Officer.

Backups of data within systems have routines to ensure database integrity, occasionally requiring systems to be taken offline for daily backups. Management Information Systems adhere to key policies, with core systems data for Human Resources, Finance, Payroll, and students retained for longer periods as necessary to meet regulatory and operational requirements.

5. SERVICE RECOVERY AND TESTING

To ensure the integrity and reliability of backup data, service recovery and testing must be conducted twice a year by our Backups Managed Service Provider (MSP). The following procedures outline the steps for effective recovery testing:

1. **Scope Agreement:**
    - The scope for each recovery test must be agreed upon with the College IT team. This includes determining whether the

test will involve selected files, entire systems, or specific data sets.

2. **Restore Scenarios:**
   - The MSP must perform various restore scenarios, including full system recoveries, incremental data recoveries, and item-level recoveries as appropriate. This ensures a comprehensive evaluation of the backup system's capabilities.

3. **Results Verification:**
   - The MSP must meticulously check the results of the restore tests for any discrepancies, failures, or performance issues. This includes verifying data integrity and assessing the time taken for recovery.

4. **Reporting:**
   - A detailed report must be provided by the MSP, documenting the testing methodology, outcomes, and any deviations from expected performance. This report should include an analysis of any issues encountered and recommendations for improvement.

5. **Follow-Up Discussion:**
   - A follow-up meeting must be held to discuss the findings of the recovery test. This meeting should involve reviewing the report, addressing any issues identified, and discussing potential areas for improvement in the backup and recovery processes.

6. **Future Testing Schedule:**
   - The next testing dates must be agreed upon during the follow-up meeting. This ensures that recovery testing remains a regular and scheduled activity, promoting continuous improvement and reliability.

By adhering to these procedures, the College ensures that its backup and recovery systems are regularly tested and verified, maintaining a high level of readiness for any data recovery needs.

6. RIGHT TO ERASURE

Edinburgh College shall maintain and enforce a ‘suppression list’ of individuals who have exercised the Right to Erasure under data protection law to ensure restores from backup do not reconstitute personal data erased previously in line with a lawful Right to Erasure request.

7. RECOVERY TIME OBJECTIVES

Following a significant outage, the IT team will aim to have any given service recovered within one working week at a maximum. Given the nature of the outage, this may be shorter or longer than specified.

8. RECOVERY PRIORITISATION

In the event of a significant outage, it is crucial to restore systems and data in a prioritised manner to ensure the continuity of critical operations. The following recovery prioritisation framework is designed as a guide to aid in the systematic restoration of services based on their importance to the College’s core functions.

Tier 1 - Critical foundational systems essential for the overall infrastructure (e.g., domain controllers, vSphere appliances, authentication services).

Tier 2 - Critical systems essential for core College operations (e.g., finance, HR, student records).

Tier 3 - Major systems supporting key educational and administrative functions (e.g., learning management systems, email services).

Tier 4 - Supporting systems and data not immediately essential but required for full operational capacity.

9. SECURITY AND ISOLATION

Data backups must be stored with a high level of security and isolation to prevent unauthorised access and ensure data integrity. The following measures must be implemented:

Encryption

All backup data must be encrypted using industry-standard encryption algorithms and encryption keys must be managed securely.

Access Control

Physical access to backup storage facilities must be strictly controlled. These facilities must be in secure data centres with 24/7 surveillance and dual access control (card and key) to ensure that only authorised personnel can enter.

Logical access to backup systems must be restricted to a limited number of authorised personnel. Access controls must include multi-factor authentication (MFA), role-based access controls (RBAC), and strict user permissions to minimise the risk of unauthorised access.

Data Isolation

Backup data must be isolated from live production environments to prevent any cross-contamination or accidental overwriting of live data. This isolation must be achieved through the use of dedicated backup storage solutions. This measure also provides robust protection against ransomware and encryption attacks, ensuring that backup data remains unaffected even if the live production environment is compromised.

Off-site backups must be stored in geographically separate locations to protect against localised disasters.

10. RESPONSIBILITIES

The Digital and Infrastructure Lead through delegated authority from the Chief Operating Officer is responsible for ensuring that back-up and data archiving is undertaken in accordance with this policy to secure College data accordingly.

11. POLICY REVIEW

This policy should be reviewed whenever affected by changes in regulatory or legal compliance, or annually, whichever is the earlier.

End of document