Policy Number	FEIT 008
Level	3
Issue	1
Issue date	07/12/2020
Review Date	15/10/2023
Author	A. Williamson
SMT approval	15/10/2020

Edinburgh College

For the future you want

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

Estates Services & IT

1. INTRODUCTION

This policy forms part of the College's Information Security Policy.

This policy is primarily concerned with backup of systems and data in relation to data security, business continuity and disaster recovery contexts. Best efforts will be made to restore data e.g. for user deleted files. Unless specifically stated otherwise, the policy relates to on-site and off-site storage as appropriate.

2. OBJECTIVES

The College, and IT team (led by the Digital Infrastructure Service Lead) specifically, are expected to:

- Follow legal, regulatory and compliance responsibilities in relation to back-up and archiving of data;
- Ensure the availability of data (that data is accessible whenever it is required by members of College staff and students and, when approved, third parties).

Ensure secure system defences are in place, and effective data management policies and procedures are at the forefront of protecting the College's data. The IT team will work with Estates services and other services departments to ensure that all necessary mitigating factors are employed to ensure the above objectives are achieved. This includes effective continuity of power supply, air conditioning and fire suppression systems.

However, in order to accomplish the above objectives, secure, reliable and robust back-up and storage facilities are required and should be effectively managed. This policy sets out the basic retention principles and periods for data held on the College's main IT systems.

3. SCOPE

This policy covers all data held by Information Services systems, which will include:

- Learning and teaching data;
- Administration and management information data;
- Centrally-held user data.

This policy does not cover data that has not been saved to the College network, or has been saved to a removable device owned by an individual or department. All College-related work should be held on the network to ensure appropriate back-ups and not directly on hard drives or removable devices which might not be backed-up.

It should be noted that back-up policies relating to third party solutions (e.g. Office 365) are reliant on 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 remote 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.

Below is a summary of the backup/archiving details:

- Backups of all data are performed daily.
- Backups are retained for 60 days before being deleted.
- Full backups are taken weekly by using synthetic backups, incremental backups are taken daily.
- Backups are run overnight, minimising impact on service provision during the day.
- Backups are retained in two alternative campus locations.
- Backups are stored in secure locations, and a limited number of authorised personnel have access.
- 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 held within systems have data backup routines which ensure database integrity is retained. Currently this means some systems are taken offline in order to back-up the data on a daily basis.
- Management Information Systems follow key policies as above, but core systems data relating to Human Resources, Finance, Payroll and students is kept for longer. Database data files of all live databases are backed up in such a way that a database can be restored to any point in time within the past month. Exports from all live databases are kept for at least 18 months, as a mixture of daily, weekly, and monthly back up. Thereafter annual (or longer) data is kept in accordance with regulatory and legal requirements.

5. SERVICE RECOVERY AND TESTING

Restores are performed on a regular basis, as needed.

Test restores of several key systems will be performed annually, during the month of July. This test will be to make sure that staff know the required procedures, and to validate the integrity of the backups.

Records of all test restores will be maintained for audit and other purposes.

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.

6. 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.

7. 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.

8. POLICY REVIEW

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