TITLE: ***DATA BACKUP POLICY***

Effective Date	20 March 2019	**Version**	01
Approved By	Management Board	**Date Approved**	20 March 2019
		Review Date	20 March 2022 *or as required*
Superseded or Obsolete Policy / Procedure(s)		**Owner**	
		IT Services	

1. Purpose of Policy

The *Data Backup Policy* has been developed to outline the importance of securing the availability of data as a critical asset of Carlow College, St. Patrick's (hereafter Carlow College). The College understands the significance of an effective data backup and recovery system to ensure data can be retrieved and recovered in the event of accidental loss or deletion or in the event of a data breach which leads to loss of data. The purpose of this Policy is to outline the secure manner in which data should be stored for successful backup and recovery. The effective use of this Policy together with the principles and guidelines outlined in this document will contribute to business continuity through implementing best practice college-wide for data backup.

2. Definitions

Data Backup is the result of copying or archiving files and folders for the purpose of being able to restore them in case of data loss

Data Owner is the person accountable for data assets in their area and authorises use of that data.

Data Processor is a third-party vendor who processes data on behalf of the data controller.

Data User is defined as a person who makes use of information for operational purposed within the College.

Full Backup is the complete backup of all files on a designated drive.

Incremental Backup only those files which have been altered since the last full backup.

Information processing is the performing of operations such as:

- obtaining, recording and retention of information;
- organising, storage, editing or adaption of information;
- retrieving or accessing information;
- communication or disclosure of information through electronic transmission; and / or
- the deletion or discarding of information.

Local Storage Device is a hard disk drive, a data storage device used for storing and retrieving digital information which is not accessible from a network.

Personal Device is a PC, Tablet, Phone, Laptop or electronic device which is personally owned by a user and not by the organisation.

Security Breach is unauthorised access to information, applications, networks or services which bypasses existing security measures.

3. Scope of Policy

This Policy applies to:

- Data Users within **all** departments college-wide who collect, store and process data on behalf of the College;
- all data held on shared locations within the Carlow College network;
- all data obtained or created as part of Research, Teaching or Administration activities by staff within scope;
- all Carlow College data stored through cloud hosted systems by third-party vendors; and / or
- third-party vendors and contractors who are considered data processors of the College who hold data on hosted servers.

When data owned by Carlow College is stored on a local storage device (on the hard drive or C: drive of a college PC or laptop) or personal devices, the user of this device must ensure that the College owned data is backed up in line with this Policy and backup guidelines. IT Services does not have the capacity to backup and recover data which is held locally; each staff member is responsible for ensuring data is backed up.

4. Policy Statement

Carlow College recognises their responsibility to ensure business continuity and access to data in the event of data loss or deletion. The College is committed to securing data by implementing best practice for the protection of data through a data backup plan enabling data retrieval. The objective of the *Data Backup Policy* is to outline the manner in which data is backed up within the College and to inform all staff of the procedures and guidelines they must follow to ensure data is being backed up appropriately. This Policy will identify best practice in line with industry recommendations which should be followed by all data users in the College. Means by which the objectives of this Policy will be reached includes backup scheduling; backup logs; backup data retention and data restore.

4.1 Backup Scheduling

The primary principles which will be used to configure backup jobs will include:

- defining specific data to be backed up;
- determining the backup type, i.e. incremental or full backup;
- the frequency and time of data backup – full backup will be run weekly; incremental backups will be run daily;
- full server system images and snapshots will be captured daily to assist recovery of systems to a particular point in time in the event of system corruption or loss; and
- the storage location for each backup to be held and the media for which the backup will be held on.

4.2 Backup Logs

Carlow College will hold and use backup logs for the following purposes:

- monitoring and auditing of all backup logs through the College backup software (Acronis);
- resolution of any issues identified in backup logs which may impact the successful completion of a backup schedule; and
- alerts to IT Officer to notify of any issues with scheduled backup jobs.

4.3 Backup Data Retention

Data arising from both incremental and full backups will be retained for at least 60 days. After this point, they will be deleted in a timeframe dependant on storage capacity and availability.

4.4 Data Restore

To ensure data backups are retrievable for restore, Carlow College will:

- run regular restore tests to ensure data which has been backed up is retrievable in its original format; and
- address any issues that may arise during restore tests and inform users where necessary of changes required to backup procedure.

Data Backup Guidelines (Appendix 1), outline the measures which will be put in place to achieve the objectives of this Policy.

5. Responsibilities

5.1 IT Services

The IT Officer is responsible for:

- developing and implementing backup procedures;
- auditing and reviewing backup logs;
- the identification and implementation of suitable security control necessary to protect and safeguard data stored, backup up and retrieved on the Carlow College network;

- the backup of all college data stored on the Carlow College network (excluding files stored on local hard drives); and
- the administration and management of centralised backup systems and storage devices.

5.2 Data Owners

Data Owners are responsible for:

- ensuring that staff within the areas they manage are using correct data management procedures in line with the *Records Management Policy*, *Information Security Policy* and this Policy; and
- Inform IT Services of any issues that may prohibit data from being included in a backup or for new data that requires.

5.3 Data Users

Data Users are responsible for:

- complying with this Policy and all other data related policies and guidelines outlined in associated documentation; and
- using best practice to protect and secure information through using appropriate backup procedures.

6. Associated Documentation

- Appendix 1: Data Backup Guidelines

Please note that the associated documentation of the 'Referenced Policies' below should also be adhered to as part of our overall quality assurance framework.

7. Referenced Policies

- *Access Management Policy*
- *Data Protection Policy*
- *Disciplinary Policy* (Staff)
- *Email and Internet Usage Policy*
- *Information and Security Policy*
- *IT Policy*
- *Records Management Policy*
- *Remote Working Policy*

8. Monitoring and Review

This Policy will be reviewed regularly and updated as necessary if and when organisational structure or business practices and processes change. Changes in data structure or information required to be included in Carlow College system backups work will also result in review and update to this Policy. All updates to this Policy and associated documents will be communicated through email to all stakeholders and a copy of all updated documentation will be posted to the Staff Gateway.

Appendix 1: Data Backup Guidelines

Data Backup Guidelines

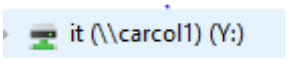
1. Responsibility for Data Backup

If you are responsible for collecting, processing or generating data on behalf of the College, you have a responsibility for ensuring that data is backed whether it is stored remotely through servers and shared network drives, or if you store it on a local device.

2. Recommended Backup Procedures

To mitigate the loss of data, the following are the recommended backup procedures to be used:

- classify your data, identifying critical data to your role which would prevent you from carrying out normal operations in the event of loss of this data;
- ensure you are including this data in a backup through the backup services provided by the College;
- if the data you use is stored in a shared network drive (e.g. below), ensure you save the file to the same location. All data stored on network drives are included in daily backups;



- backup data must be stored at a backup location that is physically different from its original creation and usage if the data is to be included in backup services provided by the College;
- College Data, which is processed on cloud hosted systems, is automatically included in system backups and therefore does not need to be isolated for further backup. Examples of these systems are:
    - Email
    - Student Record Management System
    - Moodle
    - One Drive
    - TurnItIn
    - Heritage
    - HR Online

- if you are using a separate backup procedure for data stored on a local device, please liaise with IT Services to ensure this data can be included in a retrieval and restore plan.

3. Data Selection

It is important to note that:

- all essential data and software required for the continued business operation and functionality of Carlow College must be included in system backups. The backups must also include data that must be preserved for legislative purposes; and

- information which is classed as supporting material which is required to process the information such as control files, install files, must also be backed up and retrievable in the event of corruption or loss.