TITLE: ***ACCESS MANAGEMENT POLICY***

Effective Date	10 April 2019	**Version**	01
Approved By	Management Board	**Date Approved**	10 April 2019
		Review Date	10 April 2022 *or as required*
Superseded or Obsolete Policy / Procedure(s)		**Owner**	
		IT Services	

1. Purpose of Policy

In line with GDPR legislation, Information Security and Data Protection policies, Carlow College, St. Patrick's (hereafter Carlow College) have a responsibility to ensure the confidentiality and security of data. The College understands the significance of correct use of data and the implementation of effective management controls within the College. The purpose of this Policy is to outline the secure manner in which access should be granted to users for use of data. The effective use of this Policy, together with the principles and guidelines outlined in this document, will contribute to implementing best practice college wide for granting and revoking data access as required for operational needs.

2. 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;
- all Carlow College information systems; and

- third-party vendors and contractors who are considered data processors of the College who hold data on hosted servers.

3. Definitions

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

Data Processor – user who processes data on behalf of the data controller.

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

Information processing – performing operations such as:

- obtaining, recording and retention of information;
- organising, storing, editing or adaption of information;
- retrieving or accessing information;
- communicating or disclosing information through electronic transmission; and / or
- deleting or discarding of information.

Local Storage Device – hard disk drive, a data storage device used for storing and retrieving digital information.

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

4. Policy Statement

Carlow College recognises their responsibility to ensure effective controls are in place to grant access to data where required and revoke access where no longer needed. There is a recognition of change within the organisation, where access may change to align with organisational and departmental re-structuring. The College is committed to securing data by implementing best practice for managing how access should be to various users within the College network. The objective of the *Access Management Policy* is to outline the manner in which access to data is granted within the College and how this access should be managed, audited and reviewed on an ongoing basis. 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 include: access control; access registration; account privileges; account de-registration and security.

4.1 Principles of Access Control

- All information stored within in the Carlow College network must have a data owner who is at management level. All access to data must be authorised and approved by the data owner.
- All Carlow College systems must be administrated by IT Services who are responsible for creating user accounts and managing system access which align with user accounts.
- IT Services are responsible for creation of shared folders and assigning access to these folders based on authorisation from data owner. IT Services will audit access to shared folders regularly to ensure only authorised users are granted access in the case of change to departmental structure.

4.2 Account Registration

- All access to the Carlow College network domain should be generated through a formal registration and de-registration process. Notice of account creation and removal should be carried out by IT Services on the instruction of HR, or where necessary by a line manager.
- The use of a generic group account to access information may be permitted under the following criteria:
    1. a single PC is designated to a number of different users within the same department / office; and
    2. it is a requirement within the user's role to facilitate operational needs under one generic user account (e.g. role or function sharing).
- A generic account must be authorised by a line manager where the need is identified by the said manager for group access to a network account. Where a generic account with multiple user access is no longer required, IT Services must be instructed to deactivate the account.
- Third-party access may be permitted for a legitimate business need. A temporary account within minimal access will be created by IT Services to facilitate access where required to third party users. Where access is no longer required, this account will be removed.
- Third-party access must be discussed with IT Services on a case by case basis to determine most effective and secure way to grant third party access. The final authorisation must be given by the data owner in that area.

4.3 Account Privileges

- Account rights and privileges will be granted on a required needs basis that aligns with the user's specific role rather than their status within the organisation.
- Access privileges are set on a criteria basis of least privileges initially where access is only granted to information they require to carry out their role. Access to further information may be granted or revoked on the instruction of the data owner.
- Where users require additional or further access, they must seek authorisation from the data owner, who in turn must inform IT Services of these change.
- In the event of a user changing role, their access must be reviewed to identify where access is no longer required. In these circumstances, the existing line manager must request the removal of the unnecessary account privileges

4.4 Account De-Registration

- When a user leaves the organisation or completes their studies, their account access will be immediately revoked.
- In the case of an employee leaving, IT Services will remove the user account on the day of departure by instruction of HR.

- In the event of a student deferring / withdrawing from their course, the student account will be deactivated on the instruction of the Admissions Office. Where students complete the course of study, all accounts will be removed on receipt of final exam results

4.5 Security

- Access to Carlow College user accounts must be protected by strong password authentication.
- Each user account must specifically identify the user attempting to logon and gain access to the network while also being identifiable and accountable for their activity for the duration of their active session.
- Regular audits will be carried out by IT Services on user accounts whereby the following actions may be taken for security purposes:
    1. the user is forced to change password at next logon for security purposes; or
    2. the user account may be locked after a number of consecutive logon failures.

5. Responsibilities

5.1: Data Owner

The Data Owner is responsible for:

- security, management and ownership of data within their area;
- managing access to the information systems and data held within their area;
- informing IT Services of any changes within their department which may affect access rights on user accounts;
- ensuring that this Policy and all other related policies are implemented in their area;
- ensuring that all access requests are approved using appropriate criteria in line with *Information Security Policy* and *Record Management Policy*; and
- conducting a bi-annual review of access management within there are to ensure all authorised access is up to date.

5.2: IT Services

IT Services are responsible for:

- taking appropriate action of receipt of instruction from relevant for user registration, including change of rights, password resets and de-activation of users in line with the *Access Management Policy* and *Information Security Policy*;
- restricting or removing access if a security breach is identified or suspected in line with *Information Security Policy*;
- carrying out regular audits on access rights comparing to Active Directory to ensure all users currently on the system are live and eligible for access to the College network;

- ensuring all access to shared folders is only granted through data owner authorisation; and
- identifying attempts to gain unauthorised to the College network through failed logon attempts.

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;
- protecting the security of the information for which they have access to;
- ensuring they only access accounts for which they have access to;
- ensuring all passwords provided to them are kept confidential and not disclosed to colleagues or third-parties;
- regularly changing their password to protect their account and minimise security risk; and
- reporting all suspected security breaches to IT Services.

6. Referenced Policies

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

7. 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 departmental structure or information 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.