Data Collection, Information & Management Policy

Revision: 1.0
Issued: 27th July 2021

TABLE OF CONTENTS

1. REVISION HISTORY AND APPROVAL

Revision	Nature of change	Approval	Date
1.0	First Issue	JL	27/07/21

2. COMMITMENT TO PRIVACY PRINCIPLES

2.1. It is PCI College's Strategy to ensure that learners and staff's privacy is upheld in all instances.

2.2. PCI College recognise that you care how information about you is used and shared, and the College appreciate you trusting that we will do so carefully. To better protect your privacy, we provide this Privacy Policy explaining our practices and the choices you can make about the way your information is collected and used by PCI College. The information below explains our policy regarding your privacy, both online and offline. By visiting www.pcicollege.ie or sharing personal information with the College you are accepting the practices described in this Privacy Policy.

3. GUIDING PRINCIPLES OF INFORMATION MANAGEMENT AND IT

3.1. It is PCI College's mission is to ensure all information (data) is stored in a secure environment and all members of staff are trained in data managment.

3.2. All information is maintained with industry standard precautions and measures to protect against intrusion for the protection of stakeholders.

3.3. Specific information security measures include:

- 3.3.1. Implementation of Multi Factor Authentican
- 3.3.2. Only approved Microsoft Systems are used by PCI College for Data Management and management of the Student/Learner Online Portal
- 3.3.3. Financial systems are approved by the Board of Directors for payroll and management of Learner Payment Plans
- 3.3.4. All payment systems follow SEPA guidelines
- 3.3.5. All information is Cloud based to minimise the risk of loss of data
- 3.3.6. Information stored is used to to ensure delivery of programmes
- 3.3.7. Data is analysed using a variety of means (including statistical analysis) to optimise our delivery of programmes
- 3.3.8. Information is only provided to third parties as part of the delivery, accreditation and validation of the programmes on offer
- 3.3.9. GDPR regulations are ahdeher+ed to including the reporting of any data breaches
- 3.3.10. GDPR in house training is provided on a cyclical basis
- 3.3.11. All third party external IT Support specalisits are required to sign a Non-Disclousure Agreement in supporting all data held within the Microsoft 365/SharePoint and CRM Systems

4. DATA PROTECTION

4.1. The Data Protection Act 2018 describes how PCI College must collect, handle and store personal information.

4.2. These rules apply regardless of whether data is stored electronically, on paper or elsewhere.

4.3. In compliance with legislation, inforation is collected, stored, retrieved and deleted as per our policies on Data Collection Use and Management.

4.4. The Data Protection Act is underpinned by eight important principles, which are applied to all data managed within PCI College. These determine that data must:

- 4.4.1. Be processed fairly and lawfully
- 4.4.2. Be obtained only for specific, lawful purposes
- 4.4.3. Be adequate, relevant and not excessive
- 4.4.4. Be accurate and kept up to date
- 4.4.5. Not be held for any longer than necessary

4.4.6. Processed in accordance with the rights of data subjects
4.4.7. Be protected in appropriate ways
4.4.8. Not be transferred outside the European Economic Area (EEA), unless that
4.4.9. country or territory also ensures an adequate level of protection

4.5. Data Collection
4.5.1. At the time of providing personal information, everyone will be informed directly or indirectly about the GDPR lawful basis for why the data is being collected. The lawful grounds for processing personal data are set out in Article 6 of the GDPR.

4.6. Data Use
4.6.1. Personal data is of no value to PCI College unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft.
4.6.2. Personal data held by PCI College is adequate, relevant and not excessive in relation to the purpose for which they are kept.

5. SUBJECT ACCESS REQUESTS

5.1. All individuals who are the subject of personal data held by PCI College are entitled to:
5.1.1. Copy of the Data being kept about him/her;
5.1.2. Know the purpose(s) for processing his/her Data;
5.1.3. Know the identity of any third parties to whom the College discloses the Data;
5.1.4. Know the source of the Data, unless this would be contrary to public interest;
5.1.5. Be informed of the logic/process/decision involved in processing the Data and how it affects him/her;
5.1.6. Know the reasons involved in decisions made about the Data Subject;
5.1.7. Receive a copy of any Data held in the form of opinions expressed about the individual, except where such opinions were given in confidence.

5.2. If an individual contacts the company requesting this information, this is called a *Subject Access Request*, under Section 4 of the Data Protection Acts.

5.3. Other rights under the Data Protection Acts:
5.3.1. Right to have any inaccurate information rectified or erased;
5.3.2. Right to have Personal Data taken off a mailing list;
5.3.3. Right to complain to the Data Protection Commissioner.

6. SAFETY AND SECURITY

6.1. PCI College and all its staff is aware of the security measures. This requirement may be satisfied by having appropriate training in place.

6.2. Information System
6.2.1. Information systems are required to collect, manage and provide critical information for the conduct of programmes at all levels of the institution and the operation of the intsitituion itself as per our Mission Vision and Values.
6.2.2. These systems are created and maintained with security of access and use in mind.
6.2.3. Information systems include:
6.2.3.1. Microsoft SharePoint
6.2.3.2. Microsoft Teams
6.2.3.3. PCI College Portal
6.2.3.4. PCI College Portal – Staff Area

6.2.3.5. Microsoft OneDrive

6.2.4. Information collected is for the purpose of:
- 6.2.4.1. to evaluate the quality of programme delivery and assessment practices
- 6.2.4.2. to support decision making
- 6.2.4.3. to produce reports for management
- 6.2.4.4. to produce reports for self-monitoring
- 6.2.4.5. to produce reports for planning purposes

6.2.5. Data collected will include:
- 6.2.5.1. Personal data and contact information
- 6.2.5.2. Academic results (continuous assessment, completed modues, module status etc.)
- 6.2.5.3. Awards conferred and award classifications
- 6.2.5.4. Completion rates
- 6.2.5.5. Programme monitoring data

6.2.6. In accordance with relevant legislation, information collected and stored must deemed sufficent to the above purposes and not excessive

6.2.7. Data in information systems will be processed securely with due care and in accordance with our Data Collection Use and Management Policy.

6.2.8. Senior Management is responsible for the College's information systems.

7. INFORMATION MANAGEMENT

7.1. The following overlapping QQI guiding principles underpin the Information and Data Management Policy at PCI College, this includes but is not limited to;

7.2. Data Management and criteria are aligned to the requirements outlined in the QQI Statutory Quality Assurance (QA) Guidelines, Section 8, pg 17, Information & Data Management). This requires that, the provider learner information management system is robust, comprehensive and capable of:
- 7.2.1. maintaining secure learner records for current use and historical review
- 7.2.2. providing reports required for internal quality management and improvement
- 7.2.3. generating data required for, and compatible with, external regulatory, professional or national systems as appropriate
- 7.2.4. generating statistical and other reports to meet internal and external information requirements, for example, on the QQI database of programmes and awards as prescribed by the legislation
- 7.2.5. ensuring that the database is maintained securely and that data relating to learner assessment is accurate and complete

7.3. In addition to this PCI College ensures version control requirements are in place to ensure data is clear, concise and accurate at all times, including updating records and statistical information.

7.4. Following the growth of Social Media, PCI College have introduced a subseqent Policy for Learners and Staff in this area to ensure safe and appropriate data management.

8. DATA SECURITY BREACHES

8.1. Data breaches may occur in a variety of contexts, such as:
- 8.1.1. Loss or theft of data (e.g. on a memory stick, laptop or paper records);
- 8.1.2. Inappropriate access controls (e.g. using insecure passwords);
- 8.1.3. Equipment failure;
- 8.1.4. Confidential information being left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account, leaving

documents on top of shared photocopiers);

8.1.5. Disclosing confidential data to unauthorised individuals;

8.1.6. Human error (e.g. emails being sent to the wrong recipient);

8.1.7. Hacking, viruses or other security attacks on IT equipment systems or networks;

8.1.8. Breaches of physical security (e.g. forcing of doors/windows/filing cabinets).

8.2. PCI staff must report all breaches without delay to the PCI College Data Protection Officer with the Incident Details and risks involved and will take the necessary actions.

8.3. The Data Protection Officer will review and evaluate the breach and its risk level. Under the General Data Protection Regulation, 2018, controllers are obligated to (a) notify of any personal data breach to the Data Protection Commission, unless they can demonstrate it is unlikely to result in a risk to data subjects; and (b) communicate that breach to data subjects, where the breach is likely to result in a high risk to data subjects.

9. LINKED POLICIES & PROCEDURES

Linked Policies	Assessment of Learners Policy Completion Rates Policy Confidentiality Policy Internet, Social Media and Email Policy Privacy Policy Recognition of Prior Lerning Policy Retention of Assessments Policy Transfer and Progression Policy
Linked Procedures	Assessment of Learners Procedure Data Collection, Use and Management Procedure Recognition of Prior Learning Procedure Retention of Assessments Procedure Transfer and Progression Procedure Support for Learners Procedures