Data Collection, Use and Management Procedure

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. Introduction

2.1. For day-to-day management of the College and appropriate documentation, there is a need to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with, or may need to contact.

2.2. The data protection policy & procedures ensures that PCI College:

2.2.1. Complies with data protection law and follows good practice

2.2.2. Protects the rights of staff, customers and partners

2.2.3. Is open about how it stores and processes individuals' data

2.2.4. Protects itself from the risks of a data breach

3. Responsabilities

3.1. Everyone who works for or with PCI College has some responsibility for ensuring data is collected, stored and handled appropriately.

3.2. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

3.3. However, these people have key areas of responsibility:

Role/Person	Responsibility
Applicant & Learners	Sbmission of accountable information and must be familiar with the College's GDPR policies from the learner perspectiuve.
Standards & Quality Assurance executives (acting as DPO)	Reviewing all data protection procedures and related policies, in line with an agreed schedule; Arranging data protection training and advice for the people covered by this policy; Handling data protection questions from staff and anyone else covered by this policy; Dealing with requests from individuals to see the data that PCI College holds about them (also called 'subject access requests'); Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
College Director (IT manager)	Ensuring all systems, services and equipment used for storing data meet acceptable security standards; Performing regular checks and scans to ensure security hardware and software is functioning properly; Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services; Keeping the board updated about data protection responsibilities, risks and issues.
Board of Directors	Responsible for ensuring that PCI College meets its legal obligations.
Marketing Manager	Approving any data protection statements attached to communications such as emails and letters; Addressing any data protection queries from journalists or media outlets like newspapers; Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

4. Procedures

4.1. PCI Data Collection, Information and Management procedure is linked to our Privacy Policy, and more information can be found at the website.

4.2. Data Collection

4.2.1. PCI College will collect personal data from a variety of sources. This includes:

4.2.1.1. Application & Booking – When you apply to one of our courses, we will collect personal data as necessary to offer and fulfil the services you request. Depending on the services you choose, we may require you to provide us with your name, postal address, telephone number, email address and identification information to establish a student account. In addition, we collect payment information, so we can proceed with the booking. We may require you to provide us with additional Personal Data as you use our Services.

4.2.1.2. Other information we collect related to your use of our sites or services – We may collect additional information from or about you when you communicate with us or contact our Student Services team.

4.2.1.3. Personal data that you choose to provide us in surveys and questionnaires in relation to the college and courses. We will provide you with a separate notice at the time of collection, if the use of that Personal Data differs from the uses disclosed in this Privacy Policy.

4.2.2. Also, when collecting data, all learners would be made fully aware of:

4.2.2.1. The identity of the persons who are collecting it (though this may often be implied)

4.2.2.2. To what use the information will be put

4.2.2.3. The persons or category of persons to whom the information will be disclosed

4.2.2.4. The existence of the right of access to their Personal Data

4.2.2.5. The right to rectify the Data if inaccurate or processed unfairly

4.2.2.6. Any other information which is necessary so that processing may be fair, and the Data Subject has all the information necessary in relation to the processing of their Data

4.2.3. If the information can be used in other ways, the individuals will be given the option of saying whether or not they wish their information to be used in these other ways.

4.2.4. Consent to Photographs/Video/Audio Recordings

4.2.4.1. Any photograph, video or audio recording of a person constitutes their Personal Data and is therefore, subject to the provisions of the Data Protection Acts

4.2.4.2. The explicit consent of the person and/or copy of third-parties consent, will be solicited in all instances where a photograph is taken, and a video or audio recording is made

*Third-party consent – third-party need to be able to demonstrate that the individual was fully informed, and consent was freely given

4.3. Data Use

4.3.1. PCI College staff is trained and informed that personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure. Staff receive guidelines on not saving copies of personal data to their own computers, and always accessing and updating the central copy of any data in the CRM system or the cloud.

4.3.2. PCI staff are also trained to ensure the screens of their computers are always locked when left unattended; and personal data would never be transferred outside of the

European Economic Area.

4.3.3.

4.3.4. PCI staff only access individuals data when necessary, and it is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

4.3.5. Data will be held in as few places as necessary. Staff will not create any unnecessary additional data sets.

4.3.5.1. Staff will take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

4.3.5.2. PCI College will make it easy for data subjects to update the information PCI College holds about them. For instance, via e-mail or phone contact.

4.3.5.3. Data should be updated as inaccuracies are discovered. For instance, if an individual can no longer be reached on their stored telephone number, it should be removed from the database.

4.3.5.4. It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

4.4. Subject access requests

4.4.1. *Subject Access Request* from individuals should be made by email, addressed to the Standards & Quality Assurance executives at *dataprotection@pcicollege.ie*. The data controller can supply a standard request form, although individuals do not have to use this. Individuals may be charged €6 per subject access request. The data controller will aim to provide the relevant data within 14 days.

4.4.2. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

4.4.3. PCI College has to clearly outline reasons for an access refusal based on Section 5 of the Data Protection Act.

5. SAFETY AND SECURITY

5.1. PCI College will have a written contract in place whenever it uses a processor. This contract should stipulate at least the following:

5.1.1. the conditions under which data may be processed;

5.1.2. the minimum security measures that the data processors must have in place;

5.1.3. some mechanism or provision that will enable the data controller to ensure that the data processor is compliant with the security requirement. (This might include a right of inspection or independent audit.)

5.2. Access to any Personal Data is restricted to authorized staff for legitimate purposes only.

5.3. Access to computer systems is protected and only authorized people has the right to reset passwords. PCI College staff is trained, and it is aware that is forbidden to share personal security passwords to any other person.

5.4. Physical Personal Data will be held securely in locked cabinets, locked rooms or rooms with limited access.

5.5. Any device used to deal with personal data will be protected with step validation and encryption.

5.6. PCI College staff are trained to be aware that it is forbidden to use personal devices to store Personal Data, and all data must be stored in the cloud.

5.7. All waste papers, printouts or any physical document will be shredded.

5.8. The processing of data on third party systems will be covered by contract with the supplier.

6. DATA SECURITY BREACHES

6.1. 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.

6.2. Leaners should also report any breaches noticed to PCI College without delay.

6.3. PCI College will report personal data breaches to the relevant supervisory authority, where the breach is likely to "result in a risk for the rights and freedoms of individuals. This must be done within 72 hours of first having become aware of the breach. Data processors will also be required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

6.4. PCI College, as a GDPR controller, will ensure to document any and all personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action(s) taken. This will enable the College to demonstrate compliance with the data breach notification regime to the DPC.

6.5. Subsequent to any data/information security breach, a thorough review of the incident must be made to ensure that the steps taken during the incident were appropriate and record the measures which were taken to prevent a repetition of the incident.

7. LINKED POLICIES & PROCEDURES

Linked Policies	Assessment of Learners Policy Completion Rates Policy Confidentiality Policy Data Collection, Use and Management Policy IT Support 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 Recognition of Prior Learning Procedure Retention of Assessments Procedure Transfer and Progression Procedure Support for Learners Procedures