

General Data Protection Policy (UK GDPR)

Contents:

1. Introduction
2. Definitions
3. Purpose
4. Risk Analysis
5. Scope
6. Responsibilities
7. Principles Relating to the Processing of Personal Data
8. The Rights of Individuals
9. Consent of the Data Subject
10. Other Lawful Bases for Processing Personal Data
11. Processing of Data on Criminal Convictions
12. Privacy Notices, Transparency and Control
13. Data Protection Impact Analysis
14. Data Sharing
15. Retention of Data
16. Reporting Personal Data Breaches
17. Closed Circuit Television (CCTV)
18. Complaints
19. Monitoring and Review

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

1. Introduction

- 1.1 This Data Protection Policy has been developed to ensure that Petroc fully complies with the Data Protection Act 2018. The policy emphasises the duties and obligations of every member of staff under this Act and the General Data Protection Regulation (UK GDPR) and what the College sees as good practice. Compliance with the Data Protection Act 2018 is the responsibility of all members of the College. Any deliberate breach of the Data Protection Policy may lead to disciplinary legislation being taken, access to College facilities being withdrawn, or a criminal prosecution. If there are any questions about the interpretation or operation of this policy, please contact the College Data Protection Officer, Director of Governance.

2. Definitions

- 2.1 For the purposes of this Policy the following definitions shall apply.

- **"personal data"** shall mean any information relating to an identified or identifiable natural person (the
- **"data subject"**); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.
- **"processing of personal data"** ("processing") shall mean any operation or set of operations which is performed upon personal data, whether by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
- **"personal data filing system"** ("filing system") shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
- **"controller"** shall mean the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.
- **"processor"** shall mean a natural or legal person, public authority, agency, or any other body which processes personal data on behalf of the controller.
- **"the College"** shall mean Petroc.

3. Purpose

This policy ensures compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and aligns with sector guidance issued by the

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

Information Commissioner's Office (ICO), Department for Education (DfE), and the Association of Colleges (AoC)."

It:

- enables the College to demonstrate that it fully complies with the Data Protection Act 2018
- ensures that all staff and members of the College are fully briefed on data protection issues
- informs staff of their responsibilities within the context of their job and show a line of responsibility towards implementing the Data Protection Act 2018 across the College
- clearly defines individual's rights about processing personal data and accessing personal data within the context of the legislation
- ensures that all personal data is stored securely
- gives direction and guidance for dealing with requests to access personal data
- ensures that all staff are aware of the issues surrounding the disclosure of personal data
- sets data retention periods for personal data
- informs staff of their responsibilities if a data breach, or near miss, occurs.

4. Risk Analysis

- 4.1 The maximum penalty for failing to comply with the Data Protection Act 2018 is the greater of 17.5 million Pounds or 4% of the College's annual turnover. The reputation of the College may also be damaged by non-compliance with this policy. The risk of non-compliance is monitored in accordance with the College's Risk Management Policy. Where there is a high risk that the rights and freedoms of individuals may be infringed, a Data Protection Impact Assessment will be undertaken.

5. Scope

- 5.1 This policy applies to both paper and electronic records across all formats including data processed or stored by third-party systems under data processing agreements.

It is a condition of employment that employees will abide by the rules and policies made by the College. Any failure to follow the policy can therefore result in disciplinary proceedings. Any member of staff or student, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the College Data Protection Officer initially. If the matter is not resolved it should be raised as a formal grievance.

The College is not responsible for any personal data processed by a member of staff or a student for their personal or domestic use, even where this involves the use of College equipment. The definition of personal or domestic use covers any data not concerned with their employment or studies at the College.

6. Responsibilities

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EglA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

- 6.1 The College, as a corporate body, is the Data Controller under the Data Protection Act 2018 and the Corporation Board is ultimately responsible for compliance.
- 6.2 A Data Protection Officer has been appointed who is responsible for day-to-day data protection matters and for developing specific guidance notes on data protection issues for the College.
- 6.3 All departmental managers and all those in managerial or supervisory roles are responsible for developing and encouraging good practice about the handling of personal data.
- 6.4 Compliance with data protection legislation is the responsibility of all members of the College who process personal information.

6.5 Staff:

All staff must comply with the policy. Managers are responsible for ensuring team adherence, and the DPO will conduct audits.”

- 6.5.1 The College defines staff and College responsibilities in the Human Resources Procedures - General Data Protection Regulations. Key areas covered include:

- How HR processes personal data in accordance with the data protection principles
- Individual rights
- Data security
- Individual responsibilities
- Training

- 6.5.2 The IT Department is responsible for ensuring that the College network is protected against malware and for encrypting all laptops and storage devices issued to staff. Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screensavers and manual records should not be left where they can be accessed by unauthorised personnel.

- 6.5.3 This procedure also applies to staff who process personal data off-site. Offsite processing presents a potentially greater risk of loss, theft, or damage to personal data. Staff should take particular care when processing personal data at home or in other locations outside the College campus.

6.6 Learners:

- 6.6.1 Learners must ensure that all personal data provided to the College is accurate and up to date. They must ensure that changes of address etc. are notified to the Department Admin Team who then must fill in the appropriate form. Students who use the College computer facilities may, from time to time, process personal data. If they do, they must notify the Data Protection Officer.

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

Any student who requires further clarification about this should contact their Department Administration Team in the first instance.

6.7 The Data Protection Officer:

6.7.1 The Director of Governance supported by the Data Protection team, is designated as the College's Data Protection Officer.

6.7.2 The Data Protection Officer is responsible for.

- informing and advising the College board and its employees about their obligations to comply with the Data Protection Act 2018 and other data protection laws
- monitoring compliance with the Data Protection Act 2018 and other data protection laws, including managing internal data protection activities, advising on data protection impact assessments, training staff, and arranging internal audits.
- being the first point of contact for supervisory authorities and for individuals whose data is processed
- maintaining the College's registration with the Information Commissioner
- maintaining and updating the College's Data Protection Policy
- informing the Information Commissioner if a breach of data security occurs.

6.8 Registration with the Information Commissioner:

6.8.1 The College is registered with the Information Commissioner and has an obligation as a Data Controller to notify the Information Commissioner of the purposes for which it processes personal data. Personal data must only be processed if the purpose for which it is required has been 'notified' to the Information Commissioner. It is a criminal offence to hold personal data that has not been registered.

6.8.2 A list of purposes, which have been registered by the College, is as follows:

- Purpose 1 Staff, Agent, and Contractor Administration
- Purpose 2 Advertising, Marketing, Public Relations, General Advice Services
- Purpose 3 Accounts and Records
- Purpose 4 Education
- Purpose 5 Student and Staff Support Services
- Purpose 6 Crime Prevention and Prosecution of Offenders
- Purpose 7 Provision of facilities to other groups or organisations

6.8.3 Managers are expected to familiarise themselves with the terms of the College's register entry. If any doubt exists as to whether any collecting, holding and use, or intended disclosure of personal data is within the terms of the College's register entry or the Data Protection Act 2018, then staff must discuss this with the Data Protection Officer before acting. Senior members of staff should keep the Data Protection Officer informed of nonstandard data held in their areas.

6.8.4 Individual data subjects can obtain full details of the College's data protection register entry with the Information Commissioner from the College Data

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

Protection Officer or from the Information Commissioner's website (<https://ico.org.uk/>).

7. Principles Relating to the Processing of Personal Data

7.1 Personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('**lawfulness, fairness and transparency**').
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be incompatible with the initial purposes ('**purpose limitation**').
- c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('**data minimisation**').
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased, or rectified without delay ('**accuracy**').
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. ('**storage limitation**').
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('**integrity and confidentiality**').
- g) Data shall not be retained longer than necessary for the purposes for which it was collected, in accordance with the storage limitation principle under Article 5(1)(e) of the UK GDPR

7.2 The College, as data controller, shall be responsible for, and be able to demonstrate compliance with, the principles above ('**accountability**').

8. The Rights of Individuals

8.1 The right to be informed:

8.1.1 The Data Protection Act 2018 sets out the information that must be supplied to individuals whose personal data the College holds and when those individuals should be informed. Further details may be obtained from the College's Data Protection Officer.

8.1.2 The information that the College supplies about the processing of personal data must be:

- concise, transparent, intelligible, and easily accessible.
- written in clear and plain language, particularly if addressed to a young person; and
- free of charge.

8.2 The right of access:

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

8.2.1 Under the Data Protection Act 2018, individuals have the right to obtain:

- confirmation that their data is being processed.
- access to their personal data; and
- other supplementary information

8.2.2 Access requests should be made to the College's Data Protection Officer in writing. The College will provide one copy of the information free of charge. However, we may charge a reasonable fee when a request is manifestly unfounded or excessive, particularly if it is repetitive.

8.3 The right to rectification:

8.3.1 Individuals are entitled to have personal data held by the College rectified if it is inaccurate or incomplete. Requests for rectification of data should be made to the College's Data Protection Officer in writing who will respond within one month. This may be extended by two months where the request for rectification is complex.

8.4 The right to erasure:

8.4.1 Individuals have a right to have their personal data erased and to prevent processing in specific circumstances. Requests for data to be erased should be made to the College's Data Protection Officer in writing. There are some specific circumstances where the right to erasure does not apply, and the College may refuse to deal with a request.

8.5 The right to restrict processing:

8.5.1 Individuals have the right to restrict the processing of their personal data in the following circumstances:

- a) the accuracy of the personal data is contested by the individual, for a period enabling the College to verify the accuracy of the personal data.
- b) the processing is unlawful, and the individual opposes the erasure of the personal data and requests the restriction of their use instead.
- c) the College no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise, or defence of legal claims.
- d) the individual has objected to processing pending verification whether the legitimate grounds of the College override those of the individual.

8.5.2 Requests to restrict the processing of data should be made to the College's Data Protection Officer in writing.

8.6 Data portability:

8.6.1 The College will provide personal data in a structured and commonly used format. We will also transmit personal data directly to another organisation if requested by the data subject.

8.7 The right to object:

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

- 8.7.1 An individual has the right to object.
- a) where the lawful basis for processing the personal data of an individual is based solely on the legitimate interests of the College or the performance of a task in the public interest, or the exercise of an official authority vested in the College, on grounds relating to his or her particular situation.
 - b) to the use of their personal data for direct marketing. Objections to the processing of personal data under this section should be notified to the Data Protection Officer in writing.

8.7.2 The College will not process personal data for the purposes of scientific or historical research and statistics.

8.8 Automated decision making and profiling:

8.8.1 The College will not undertake automated decision making or process personal data for the purpose of profiling individuals.

9. **Consent of the Data Subject**

9.1 The College will identify and record a lawful basis for the processing of personal data.

9.2 The lawful basis for the processing of personal data will normally be the consent of the data subject. Consent must be a freely given, specific, informed, and unambiguous indication of the individual's wishes. Consent will not be inferred from silence, pre-ticked boxes, or inactivity. Consent is not required if a different lawful basis has been identified (see following section). Individuals may withdraw their consent for the processing of their personal data by notifying the Data Protection Officer in writing.

10. **Other Lawful Bases for Processing Personal Data**


- 10.1 Having regard to the purpose of the data processing and the relationship with the individual, the College may determine that it is not appropriate to obtain the consent of the data subject and may instead identify and document one of the following lawful bases for the processing of personal data:
- a) the processing is necessary for a contract between the College and the individual, or because the individual has asked the College to take specific steps before entering a contract
 - b) the processing is necessary for the College to comply with the law, for example, The Further and Higher Education Act 1998
 - c) the processing is necessary to protect someone's life
 - d) the processing is necessary for the College to perform a task in the public interest or to discharge its official functions, and the task or function has a clear basis in law
 - e) the processing is necessary for the legitimate interests of the College or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests (this does not apply if the College is processing data to perform its official tasks).

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

11. Processing of Data on Criminal Convictions

- 11.1 To comply with statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the College obtains details of criminal allegations, proceedings, and convictions for the purpose of safeguarding the young people and vulnerable adults for which it is responsible. This data is only retained for as long as required for this purpose and is then deleted. The College does not keep a comprehensive register of criminal convictions.

12. Privacy Notices, Transparency and Control

- 12.1 The College aims to comply with the code of practice on communicating privacy information to individuals issued by the Information Commissioner's Office. Privacy notices will be as informative as possible and will, as a minimum, inform individuals:
- that the College is the data controller
 - how their personal data will be used by the College and  with whom their data will be shared.
- 12.2 Privacy information will be given before personal data is collected and may be communicated through a variety of media:
- in writing - forms, such as application forms; printed media; printed adverts
 - electronically - on the College website; in emails; in text messages; in mobile apps
 - orally - face to face or when speaking on the telephone (this will be documented)
 - through signage - for example an information poster in a public area.

13. Data Protection Impact Analysis

- 13.1 The College aims to comply with the code of practice on conducting privacy impact assessments issued by the Information Commissioner's Office.
- 13.2 Risks created by the College's data processing activities are continuously monitored through the College's risk register to identify when a type of processing is likely to result in a high risk to the rights and freedoms of individuals. This is most likely when any of the following conditions are present:
- sensitive data or data of a highly personal nature
 - data concerning vulnerable data subjects
 - data processed on a large scale
 - applying new technological or organisational solutions.
- 13.3 Where the likelihood that the rights and freedoms of individuals may be infringed is assessed as 'High' or above (using the College's methodology for scoring risks), the Data Protection Officer will arrange for a Data Protection Impact Assessment to be undertaken. The Data Protection Impact Assessment will incorporate the following steps:
- describe the information flows
 - identify the privacy and related risks
 - identify and evaluate the privacy solutions
 - sign off and record the assessment outcomes
 - integrate the outcomes into the existing processes or project plan

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EglA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

- consult with internal and external stakeholders as needed throughout the process.

14. Data Sharing

- 14.1 The College aims to comply with the code of practice on data sharing issued by the Information Commissioner's Office.
- 14.2 The College will inform an individual if it intends to share his or her personal data with another organisation and will normally obtain the consent of the individual.
- 14.3 The College does not require the consent of a student to share his or her personal data for the purpose on complying with:
- its contractual obligations to the Education and Skills Funding Agency and successor organisations
 - its legal obligations under the education acts and safeguarding legislation.
- 14.4 The College may share personal data without the individual's knowledge, where, for example, personal data is processed for the:
- prevention or detection of crime
 - apprehension or prosecution of offenders or
 - assessment or collection of tax or duty.
- 14.5 The College will share personal data with its service providers to the minimum extent required for those service providers to discharge their obligations to the College under relevant service contracts. Service providers, not limited to, but may include auditors, payroll & HR system providers, bankers, debt collection agencies, software suppliers and funding providers.
- 14.6 The Data Protection Act 2018 states that the safeguarding of children and individuals at risk are a processing condition that allows practitioners to share information.
- 14.7 The College will not transfer personal data outside the protection of the UK GDPR, unless the rights of the individuals in respect of their personal data is protected in another way, or one of a limited number of exceptions is applied.

15. Retention of Data

- 15.1 The College will retain data in a form which permits the identification of data subjects for no longer than the purposes for which the data are processed. The retention periods for each class of data are shown within the Document Retention and Disposal Policy.

16. Reporting Personal Data Breaches¹

- 16.1 A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This is more than a loss of personal data. All personal data breaches, or circumstances which may give rise to a personal data breach, must be reported to the Data Protection Officer immediately. The Data Protection Officer will investigate the

¹ The procedure for staff reporting a data breach can be found in Appendix 1

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

alleged breach and prepare a written report for the Principal and Chief Executive Officer.

- 16.2 If, in the opinion of the Principal and Chief Executive Officer and the Data Protection Office, the breach is likely to result in a risk to the rights and freedoms of individuals (if unaddressed, such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage) then the Data Protection Officer will notify the Information Commissioner. This must occur within 72 hours of the college becoming aware that a breach has occurred. This will be the first point of contact within the college, not when the incident is reported to the DPO.
- 16.3 When considering if the incident constitutes a Personal Data Breach the DPO will look at the following:
1. Can the data broadly be defined as a security incident that has affected the confidentiality, integrity, or availability of personal data?
 2. Does the breach involve the personal data of living individuals?
 3. Can the individual/individuals involved in the breach be clearly identified?
 4. The severity level of the potential impact on individuals as a result of the breach and the likelihood of this happening.
- 16.4 If, in the opinion of the Principal and Chief Executive Officer, the breach is likely to result in a high risk to the rights and freedoms of individuals, then the Data Protection Officer will, in addition to notifying the ICO, make arrangements to notify the individuals concerned.

17. Closed Circuit Television (CCTV)

- 17.1 Petroc takes data privacy seriously and understands the importance of respecting individual privacy rights of learners, staff, and visitors to its campuses. As such, the college uses CCTV cameras in public spaces around its campuses, for the purpose of ensuring public safety and preventing criminal activity. The captured data is securely stored and accessed only by authorised personnel who have been trained to handle sensitive information.
- 17.2 Petroc has taken necessary measures to ensure that the CCTV footage is not used for any other purpose than what is intended and is deleted after a reasonable time. The college aims to ensure that notices are displayed to inform campus users about the presence of CCTV cameras, the purpose for which they are used, and contact information to exercise their rights. Measures include:
- any monitoring of data will be carried out only by a limited number of specified staff
 - data will be accessed only by the Leads in Safeguarding and Estates in the first instance
 - personal data obtained during monitoring will be erased as soon as possible after any investigation is complete
 - data will only be made available to law enforcement agencies involved in the prevention and detection of crime, and no other third parties

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

- staff involved in monitoring will maintain confidentiality in respect of personal data
- data are securely stored, where only a limited number of authorised persons may have access to them
- the operating equipment is regularly checked to ensure that it is working properly (e.g. the recording media used is of an appropriate standard and that features on the equipment, such as the date and time stamp, are correctly set and applied to the data).

17.3 Individuals have the right to access their personal data through subject access requests, or to request its deletion or correction if needed by writing to the college's Data Protection Officer at dpo@petroc.ac.uk.

18. Complaints

18.1 Any person who believes that the College has not complied with this Policy, or with any aspect of the wider Data Protection Act 2018, should notify the College's Data Protection Officer in the first instance. If the issue is not resolved, a complaint should be made in writing to the Executive Office, Petroc, Old Sticklepath Hill, Barnstaple, EX31 2BQ and will be investigated in accordance with the College's Complaints Resolution Procedure.

18.2 If the complainant is still unhappy with the College's response or needs any advice he or she should contact the Information Commissioner's Office (ICO) on the ICO helpline (telephone: 0303 123 1113) or go to the Information Commissioner's website at <https://www.gov.uk/data-protection/make-a-complaint>.

19. Monitoring and Review

19.1 The Data Protection Officer is responsible overall for the implementation of the Policy.

19.2 As a rule the Policy will be reviewed every two years. However, Petroc reserves the right to amend the policy at its discretion and in accordance with the relevant legal regulations/laws.

19.3 The policy will be approved and monitored through the Full Governing Board.

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

Appendix 1 : Data Breach Procedure

Data breaches can happen at any organisation, including colleges. A data breach refers to the unauthorised or accidental access, disclosure, or loss of personal data. Under the UK General Data Protection Regulation (GDPR) and the 2018 Data Protection Act (DPA), a data breach can include a range of incidents, such as:

- A cyber-attack on a computer system.
- The loss of physical documents containing personal data; or
- The accidental sending of personal data to the wrong recipient.

In all cases, organisations must take prompt action to identify the breach, assess the risk to individuals whose data has been compromised, and take appropriate steps to mitigate any potential harm. Additionally, under the UK GDPR and DPA, organisations are required to notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of a data breach, unless it is unlikely to result in a risk to individuals' rights and freedoms.

It is important to refer to the following Data Breach Procedure in instances where college staff, learners or visitors are concerned that a data breach has occurred.

1. Identify and Inform:

The first step is to identify the breach as quickly as possible, and to inform the college's Data Protection Team, including the Data Protection Officer, immediately should a potential data breach occur. Information should be supplied to give context, including - for example - time of data breach, those affected, and the type of data involved.

2. Assess the impact:

Once the breach has been contained by appropriate teams, for example IT, the college's Data Protection Officer alongside the Data Protection Team, will assess the impact of the breach. This will involve determining what data has been accessed, the number of individuals affected, and the potential risks to individuals because of the breach.

3. Notify affected individuals:

If the data breach poses a risk to individuals, they must be notified as soon as possible with guidance from the college's Data Protection Officer. Notification will include details of the breach, the steps being taken to address it, and advice on how to protect themselves. The Data Protection Officer should draft the

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body

notification and work with relevant departments to ensure it is delivered to all affected individuals.

4. Notify the Information Commissioner's Office (ICO):

If the breach is significant, Petroc must notify the ICO within 72 hours of becoming aware of it. The Data Protection Officer will submit the notification, which should include details of the breach, the number of individuals affected, and the steps being taken to address it.

5. Review and learn from the breach:

After the breach has been addressed, it is important for any organisation, including Petroc, to review the incident and identify any areas for improvement, using guidance provided from the Data Protection Team. This may involve reviewing security policies, procedures, and training. Lessons learned should be documented and shared with relevant staff and departments.

6. Prevent future breaches:

In the event of a data breach, Petroc will take every possible step to help prevent future breaches. This may include strengthening security measures, conducting additional security audits, and providing further training to staff and students on data protection.

The Data Protection Officer should be the primary point of contact for all data breaches and can be reached at dpo@petroc.ac.uk.

Policy Name: General Data Protection Policy	Policy No: P11006
Approved Date: July 2025	Review Date: July 2027
Approved by: Full Governing Body	EqlA Completed: Yes
Author: Director of Governance	Monitoring & Evaluation: Full Governing Body