dŜƨŜŮıɲ Bıžı âŮYžŜŎžbYƨ âY]bÔÛ ϰĂ¥ dBâåΨ

;YƨžŜƨžāz

1. Introduction

`. rzŽŮYŕpŎžbYz

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of the Data Protection Policy may lead to disciplinary legislation being taken, access to College facilities being withdrawn, or a criminal prosecution.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, Governance Advisor.

´. BŜÅzbžbYa

- inform staff of their responsibilities within the context of their job and show a line of responsibility towards implementing the Data Protection Act 2018

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:

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 Services 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 a

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 [illegible].1

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. Lawful Basis for Processing

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. Legitimate Interests Basis

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).

11. Criminal Allegations, Proceedings and 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 req adults f a

`´ â Ŭ ô ı Ŏ Û ´ Y ʒ

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. Storage and Retention

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. Personal Data Breach Notification[3]

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 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

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

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 Principals PA, Petroc, Old Sticklepath Hill, Barnstaple, EX31 2BQ and will be investigated in accordance with the College's Complaints Resolution Procedure, a copy of which may be obtained from Reception.

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 Policy 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 with to