INTRODUCTION

The College holds personal data about learners and citizens, employees, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

DEFINITIONS

Business Purposes

The purposes for which personal data may be used by us are personnel, administrative, financial, regulatory, payroll and business development purposes.

Business purposes include the following:

- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information and security vetting
- Investigating complaints
- Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments
- Monitoring staff conduct, disciplinary matters
- Marketing our business
- Improving services

Personal Data

Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts.

Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV.

Sensitive Personal Data

Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, genetic or biometric data, information relating to sex life or sexual orientation criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

DATA PROTECTION PRINCIPLES

The holding and processing of personal information on staff and students *(Note: the term Student includes Portland Freedom Citizens for the purposes of this Procedure),* must be in accordance with Data Protection Act principles. These are personal data items and must be:

- Fairly and lawfully and transparently obtained and processed
- Processed for particular lawful purposes and not in any manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate and kept up to date
- Not kept for longer than is absolutely necessary
- Secure from unauthorised access, accidental loss or destruction

Portland College must be able to demonstrate compliance with these principles

FAIR AND LAWFUL PROCESSING AND CONSENT

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

In most cases we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to be freely given, informed and must be an explicit opt in. It should clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Consent must be able to be withdrawn in straightforward manner and may need to be periodically refreshed.

The data protection principles must be followed when deciding what data is processed, how much data is retained and for how long it is kept.

MAKING A DATA SUBJECT REQUEST (SAR)

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. All subject access requests should be referred immediately to the DPO.

Staff should contact the Data Protection Officer if they would like to correct or request information that is held about them. There are also restrictions on the information to which subjects are entitled under applicable law.

The SAR response must be processed within one month and the copy of data received in a structured common electronic format. This an include transfer directly onto another system.

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

PRIVACY BY DESIGN AND DEFAULT

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

PROCESSING DATA FOR DIRECT MARKETING AND FUNDRAISING PURPOSES

Staff should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.

Staff should not send direct marketing material to someone electronically (e.g. via email) unless they have an existing business relationship with them in relation to the services being marketed.

Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.

DATA SECURITY

Personal data must be stored securely to prevent loss or misuse. Where other organisations process personal data as a service on behalf of the college, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it

- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed in accordance with IT procedures.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

DISCLOSING PERSONAL DATA

Personal data should not generally be disclosed to third parties without the permission of the individual concerned. In this context, "third parties" includes family members, friends, local authorities, government bodies and the police, unless disclosure is exempted by the GDPR or by other legislation. Under certain circumstances, data may however be released. Note that among other circumstances the Act permits release of data without express consent:

- for the purpose of protecting the vital interests of the individual (e.g., release of medical data where failure to do so could result in harm to, or the death of, the individual)
- for the prevention or detection of crime
- for the apprehension or prosecution of offenders
- for the discharge of regulatory functions, including securing the health, safety and welfare of persons at work
- where the disclosure is required by legislation, by any rule of law, or by the order of a court.

Most bodies that may request personal data in such circumstances should be able to provide documentary evidence to support their request. In case of doubt the request should be referred to DPO.

RESPONSIBILITIES OF STAFF AND STUDENTS

The College expects all its staff and students to comply fully with this Data Protection Policy. Disciplinary action may be taken against any employee or student who breaches any of the instructions or procedures following from this Policy.

Members of staff are responsible for:

- ensuring that any information they provide to the College in connection with their employment is accurate and up-to-date
- informing the College of any errors or changes to information which they have provided (e.g. change of address)
- checking the information the College sends out from time to time giving details of information kept and processed about staff

Students must likewise ensure that any information they provide to the College is accurate and is kept up-to-date. If they find themselves in a position where they are processing personal data about staff or other students (e.g., as a student representative on a College committee or group, or as the secretary of a society), they must ensure that they comply with College Policy and with the requirements of the Act.

Ian Cowin

Assistant Principal Corporate Services and

Data Protection Officer