# Data Protection Policy

| | |
|---|---|
| **Reviewed**:<br>November 2024 | **Next review due**:<br>November 2027 |
| **Approving Body**:<br>Corporation | **ELT contact**:<br>Chief Financial Operations Officer |
| **Date approved:**<br>16 December 2024 | **Author:**<br>Data Protection Officer |

* This procedure may need to be reviewed before the review date stated, to reflect changes in government and other agencies' advice, guidance and legislation.

# Contents

# 1. Introduction

City College Plymouth (the 'College') is a leading provider of vocational, professional and technical training in the South West, that strives to provide a learning environment and organisational culture that impacts positively on the health, wellbeing and sustainability of our community, to enable all our students and staff to achieve their full potential.

The term 'College Community' includes all students, staff, governors, parents/carers, volunteers and visitors.

**Our vision:**

- The learning destination of choice

**Our core values:**

- Respect
- Ownership
- Integrity

# 2. Our commitment

City College Plymouth is committed to protecting the privacy of personal information of all College users. The College's reputation and future growth is dependent on the way the College manages and protects personal data, both internally and externally.

Protecting the confidentiality and integrity of personal data is a key responsibility for **everyone** within the College.

As well as being good practice, the General Data Protection Regulation 2018 (GDPR) imposes new, stricter legal requirements on collecting and processing personal data with greater transparency required and severe sanctions for data breaches and non-compliance.

# 3 Policy statement

This policy applies to all members of College staff.

This policy applies to all personal and special category information as defined by the GDPR, whether it is processed electronically, on paper or by other mediums.

The College has appointed the Chief Financial Operations Officer as the Executive Leadership Team member responsible for ensuring that data is collected, held and processed in accordance with the GDPR 2018.

A Data Protection Officer (Data Protection Officer) has been appointed who will be the day to day primary contact for data protection issues, ensuring compliance, dealing with data subject requests, making appropriate reports and audits and ensuring the College maintains and demonstrates compliance regarding data protection matters.

All members of staff are individually responsible for complying with this policy and procedures and for enabling students to do so.

Staff and students will be made aware of the UK Data Protection Laws and this policy. They will be given guidance on complying with it and be informed of the consequences of failing to

do so.

New College personnel will receive a copy of this policy when they start and may receive periodic revisions of this policy.

This policy will be reviewed every three years, although the College reserves the right to make changes to the policy and procedures at any time.

All members of the Executive Leadership Team, Directors and College Leadership Team are primarily responsible for ensuring all aspects of this policy are carried out effectively within their areas of responsibility (including cross college responsibilities).

Any queries or issues concerning this policy, its wording or implementation, should be directed to the College Data Protection Officer who has day to day responsibility for ensuring the College's compliance with this policy.

# 4 Objectives

The objective of this policy is to set out the basis on which the College will collect and use personal data both where the College collects it from individuals itself or where it is provided to the College by third parties. It also sets the rules and procedures on how the College handles, uses, transfers and stores personal data to ensure the privacy and interests of individuals can be protected.

This policy will demonstrate the College's application of its responsibilities under the GDPR, in particular, the principles underpinning the GDPR.

This policy will explain the security measures, controls and other policies the College has implemented to protect and secure its data and to mitigate risks of a data breach.

The policy will set out the rights afforded to individuals under the GDPR, including the right to request data and to complain to the College or the ICO.

The policy will explain the procedure where there has been a data breach.

The policy will also set out the College's policy for deciding upon the retention of personal information, specific details of which will be recorded in the College Information Asset Register.

# 5 Associated policies and documentation

This data protection policy should be read in conjunction with the following College policies:

- Procedures for Data Protection, including Impact Assessment, Information Requests and Breach Notification and Management
- Information Security policies
- Social Media guidelines
- Home Working policy

# 6 Staff responsibilities

All College staff including outsourced suppliers must comply with this policy.

College staff must ensure that they keep confidential all personal data they collect, store, use

or come into contact with during the performance of their duties, including information communicated verbally.

College staff are responsible for ensuring that any personal data about them and supplied by them to the College is accurate and up to date.

College staff must not release or disclose any personal data (including by phone calls or verbally):

a) Outside the College; or

b) Inside the College to College personnel not authorised to access the personal data without specific authorisation from the Data Protection Officer.

College staff must take all steps to ensure there is no unauthorised access to personal data, whether by other College staff who are not authorised to see such personal data or by people/organisations outside the College.

Any request from a student or other individual exercising their data rights, eg for access, erasure, rectification or objection etc, must be referred to the Data Protection Officer as soon possible and in any event within 24 hours of receiving the request. Staff must not make any attempt to deal with or respond to any data request without authorisation from the Data Protection Officer. For more information on responding to data requests, refer to the Data Request Procedure.

Any breach or failure to comply with any part of the data protection policy or linked policies and procedures may be dealt with under the College's Disciplinary policy.

# 7 College responsibilities

City College Plymouth is a data controller and a data processor.

Executive Leadership Team, Directors, College Leadership Team and all those in managerial or supervisory roles throughout the College are responsible for developing and encouraging good data handling practices within the College; responsibilities are also set out in individual job descriptions.

The Data Protection Officer and a member of the Executive Leadership Team are accountable to the College's Board of Governors for the management of personal information within the College and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes development and implementation of the GDPR as required by this policy and also security and risk management in relation to compliance with this policy.

The Data Protection Officer, who the Board of Governors considers to be suitably qualified and experienced, has been appointed to take responsibility for the College's compliance with this policy on a day to day basis and in particular, has responsibility for ensuring that the College complies with the GDPR 2018, as do all managers in respect of data processing which takes place in their area of responsibility.

The Data Protection Officer has specific responsibilities in respect of individuals exercising their rights or making a Subject Access Request (SAR) and is the first point of contact for staff seeking clarification on any aspect of the data protection compliance.

# 8 College registration with the ICO

The College has notified the Information Commissioner's Office (ICO) that it is a data controller and data processor and that it processes personal information about individuals.

A copy of the College's ICO registration certificate is retained by the Data Protection Officer and is available on Staff Central in the Legal and Insurance library.

The College's current ICO registration number is **Z4941564**. Registration will be reviewed annually by the Data Protection Officer.

# 9 Publication of College information

Information which is already within the public domain is exempt from the provisions of the GDPR and as such, may be disclosed to third parties without requiring the consent of a data subject.

'Public domain' will include reference to information which is freely available worldwide upon the Internet.

It is College Policy to make the following information available to the public for inspection:

- Names of Governors;
- Staff Names (including via ID Cards);
- Staff job titles;
- Staff email addresses;
- Staff work contact numbers

The Executive Leadership and College Leadership Team Charts (with photos) are not dealt with as a public document, but names, job titles and contact details can be replicated and placed in the public domain.

The College Intranet is not considered to be within the public domain.

# 10 GDPR principles

The College is committed to complying with the GDPR 2018 and all staff must ensure personal data is held and processed in accordance with the data protection principles as set out in Article 5 of the GDPR.

The College's policies and procedures are designed to ensure compliance with these principles. The principles of GDPR state that an individual's personal information must:

- be processed lawfully, fairly and transparently
- be obtained only for specific, lawful purposes
- be adequate, relevant and not excessive
- be accurate and kept up-to-date
- not be held for any longer than is necessary

- be processed in accordance with the rights of the individual
- be protected by appropriate security measures
- not be transferred outside the European Economic Area, unless that country or territory also ensures an adequate level of data protection

Staff are to refer to the Data Protection Officer if further clarification of any of these principles is required.

## 11 Demonstration of compliance with the principles of GDPR

The College and its users promote compliance accountability and governance of the GDPR principles.

The College will demonstrate compliance with the principles in many ways including implementing data protection and other information security policies, adhering to relevant Codes of conduct, providing training and awareness, implementing technical and organisational security measures, as well as adopting techniques such as data protection by design, privacy notices, data protection impact assessments (DPIAs) and by the appointment of a Data Protection Officer.

## 12 Lawful basis

College staff must ensure there is a lawful basis for collecting, processing and retaining personal data and that data is only used for the basis originally intended.

The main lawful purposes used for processing personal data are that:

- it is necessary for the performance of a contract
- it is necessary for compliance with a legal/statutory obligation
- it is necessary for performance of a task carried out in the public interest
- it has been consented to by the individual

Where the data being processed is “special category data”, an additional lawful basis must also be established. These additional purposes include:

- substantial public interest
- explicit consent
- employment and social security obligations
- vital interests
- necessary for establishment or defence of legal claims

**Consent**

If consent is being used as the lawful basis, it must be freely given, specific, informed and unambiguous, with positive, affirmative action by the individual signifying agreement to the processing of their personal data. The individual can withdraw their consent at any time (although if another lawful basis or an exemption exists, processing may still be permitted and disclosure made without consent).

Where the individual is not considered competent to provide informed consent, processing must be authorised by the individual's guardian/next of kin.

Where the individual is a child under 13 years of age, consent for processing must be obtained from the person with parental responsibility or other authorised person.

The GDPR 2018 permits certain disclosures to be made without the consent of the individual. Disclosure may be made without consent where the information is requested for one or more of the following purposes:

- To safeguard national security
- To prevent or detect crime including the apprehension of offenders
- To assess or collect tax/duty
- To discharge regulatory or statutory obligations, including the health, safety and welfare of individuals
- To prevent serious harm to a third party
- To protect the vital interests of the individual, such as life and death situations

All requests to disclose data for one of the following non-consent reasons must be supported by appropriate paperwork and all such potential disclosures must be reported to and specifically authorised by the College's Data Protection Officer.

**Marketing**

The College will sometimes contact individuals to send them marketing information or to promote the College. Where the College carries out any marketing activity, it will only do so in a legally compliant manner. In particular, the College will require clear affirmative action from individuals, positive opt in and/or consent before carrying out marketing activities.

In addition to complying with the GDPR in relation to marketing, the College also complies with the Privacy and Electronic Communications Regulations 2003 (PECR).

Any questions or issues regarding the lawful basis for processing must be referred in the first instance to the Data Protection Officer.

**Images and Recordings**Where the College collects images and/or recordings and individuals may be identified in those images, arrangements for collection, storage and disposal will be carefully considered based on the basis for processing. In some cases, arrangements for the security or sharing of media, for example, may differ from standard procedures. In particular, the College will:

- Ensure that all images of students and members of the public collected for marketing and communication purposes are supported by clear and informed consent, which may be amended or withdrawn by the individual at any time. The group will ensure that individuals are aware of the limitations of their right to restrict processing in relation to images already published in digital or paper form and will involve individuals in the approval process for any use of their image which might have a significant public reach or impact.
- Ensure that CCTV images and recordings are collected, stored and used within a secure environment, in accordance with the published procedures and codes of conduct.

- Use images and recordings created as part of the teaching, learning and assessment process only to provide access and support to students as part of their learning programme. This may include the recording of lessons and other activities, which may include images of students, teachers and other staff. Such images and recordings will be shared with staff and students via the agreed Digital Learning Platform(s) and therefore subject to specific, more open arrangements for security and retention.

Images and recordings of staff created for the purposes of delivering teaching, learning and assessment through online platforms, or to create reusable teaching and learning resources, will be separately classified and subject to specific criteria for retention and re-use.

## 13 Privacy notices and transparent processing

Where the College collects and processes personal information regarding individuals, the College will inform the individual about how the College uses their personal data. This will be done primarily by way of privacy notices.

Privacy notices are displayed on the College Website to ensure privacy information is transparent and accessible to students and staff.

All staff must ensure they read and comply with the appropriate privacy notices.

Staff must refer any request by an individual to exercise their rights, for example, a request for access or for erasure, to the Data Protection Officer as soon as possible in the first instance. No disclosure of data is to be made by staff without the prior approval of the Data Protection Officer.

## 14 Rights of data subjects

The College fully recognises and respects the rights given to individuals under the GDPR 2018.

The College ensures that individuals are made aware and may exercise their rights. These rights are contained in the College's privacy notices and are also summarised below.

The procedure for dealing with a data request is contained in the Data Request procedure.

Any queries or requests regarding these rights must be directed to the Data Protection Officer as soon as possible in the first instance. College staff must not attempt to deal with or respond to any data request or request relating to these rights without authorisation from the Data Protection Officer.

**An individual has the following rights relating to their data under the GDPR:**

**Right to be informed**

An individual may ask the College what personal information it is holding, whether electronically, on paper or on other mediums.

**Right of access/subject access request**

An individual may ask the College for a copy of their personal information held by the College. This will be provided free of charge except where a request is manifestly unfounded, excessive or repetitive, in which case a reasonable fee can be charged, based on the administrative cost of providing the information.

The College will aim to supply the information to the individual within one month from receipt of the request, although there are circumstances where this time may be extended.

**Right to rectification**

An individual has the right to ask the College to rectify any personal data if it is inaccurate or incomplete. If the College has disclosed personal information to third parties, the College will inform the third party of the rectification where possible.

**Right to erasure/right to be forgotten**

An individual has the right in certain circumstances, such as where the College's use of your personal information is based on consent and the College has no other legal basis to use the personal information, to ask the College to delete their personal information.

**Right to restrict processing**

An individual has the right in certain circumstances, such as where the College no longer needs the personal information, to request that the College restricts its use of their personal information.

**Right to data portability**

An individual has the right where processing is based on consent or the performance of a contract and is carried out by automated means, to ask the College to provide them with a copy of their personal information in a structured, commonly used, machine readable format.

**Right to object**

Where processing has been based on legitimate interests, the performance of a task in the public interest or for direct marketing purposes, an individual can object to the processing. The College, however, may still continue to process and hold the personal information if it can demonstrate legitimate grounds for processing it, for example, the processing is for the establishment, exercise or defence of legal claims or for evidential reasons.

**Right to complain**

If an individual has any questions about their personal information or the way in which their information is being used or processed by the College, they should contact the College's Data Protection Officer at:

Data Protection Officer

City College Plymouth, Kings Road, Devonport, Plymouth, PL1 5QG

01752 305735

dpo@cityplym.ac.uk

If an individual wishes to complain about how their complaint was handled or appeal against any decision made following a complaint, they may lodge a further complaint via the College's Talkback complaint procedure.

This can be done by:

Emailing: talkback@cityplym.ac.uk

Telephone: 01752 305285

Writing to: The Talkback Team at City College Plymouth.

Further details can be found on the College website.

In addition, individuals have the right to complain to the Information Commissioners Office (ICO), the supervisory authority for data protection matters.

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

0303 1231113 or 01625 545745

casework@ico.org.uk www.ico.org.uk

## 15 Automated Decision Making and Profiling

Any automated decision making or profiling carried out by the College can only be done once the Executive Leadership Team is confident that it is complying with Data Protection laws. Any staff wishing to carry out automated decision making or profiling must inform the Data Protection Officer who will co-ordinate the completion of a comprehensive DPIA to evaluate the risks associated with the proposed processing activities. Staff must not carry out automated decision making profiling without the prior approval of the Data Protection Officer.

## 16 Data requests/Subject Access Requests (SARs)

The College fully recognises and respects the above data rights given to individuals under the GDPR and will ensure that individuals may exercise those rights where appropriate.

If a member of staff receives a request from an individual to exercise any of the rights set out in this policy, that member of staff **must:**

- Inform the Data Protection Officer as soon as possible and in any event, within 24 hours of receiving the request.
- Inform the Data Protection Officer what the request consists of, who has made the request and provide the Data Protection Officer with a copy of the request.
- Not make any attempt to deal with or respond to the request without authorisation from the Data Protection Officer.

The Data Protection Officer will then deal with the request, contact the individual and respond accordingly, following the Data Request procedure.

Please note, the College must reply within one month of receiving any data request, so prompt reporting is essential to allow time for the Data Protection Officer to consider the request and sufficient time for the College to obtain the data from various College systems and sources.

## 17 Data security

The College and its staff take information security extremely seriously in order to protect the privacy of individuals and to ensure compliance with the GDPR.

The College has numerous security measures, policies and procedures to prevent or mitigate unlawful or unauthorised processing of personal data, accidental loss of, or damage to, personal data.

All College staff are responsible for ensuring that any personal data the College holds and for which they are responsible is kept securely and is not disclosed without lawful authority or consent.

The College and its staff use appropriate technical and organisational measures to protect personal data and to mitigate the risk of a data breach. These measures include:

- Password protection
- Automatic locking of idle computer terminals
- Virus and Malware checking software and firewalls
- Encryption of devices
- Security of local and wide area networks
- Privacy enhancing technologies such as pseudonymisation and anonymisation
- Identifying appropriate international security standards relevant to the College
- External security certification such as Cyber Essentials
- Lockable rooms with controlled access
- Lockable filing cabinets/lockable drawers
- Adoption of a clear desk policy
- Adhering to the Bring Your Own Device (BOYD) policy
- Restricting access of data and systems only to those who have professional need of it
- Making regular backups of personal data
- Deletion or disposal of personal data only in accordance with the College retention policy-disposal of manual records securely and confidentially; erasure/removal of computer hard drives before disposal
- Pre-employment checks
- Due diligence on external contractors and partners, written data sharing agreements and checking of data protection policies / security measures
- Appropriate training for College staff
- Inclusion of data protection obligations in the staff code of conduct
- Robust disciplinary processes
- Monitoring of security policy compliance

- Information and system security measures contained in associated policies such as the Information security, IT security, BOYD, computing and digital equipment acceptable use and other policies

In addition, the College has appointed a Data Protection Officer who, amongst other duties, will review security measures, ensure adherence to policies, carry out internal audits, undertake data protection impact assessments (DPIAs), carry out sufficient due diligence on contractors and other third parties, deal with data requests from individuals exercising their rights and oversee any data security breach/notification.

## 18 Disclosure of data by staff

As referred to in section 5, all College staff must ensure that personal data is not disclosed to third parties, including family members, friends and public bodies, without appropriate authority.

All staff must exercise caution when asked to disclose any personal information to anyone other than the confirmed data subject and must consult the Data Protection Officer.

Staff must contact the Data Protection Officer for advice and authority before any access or disclosure is given or agreeing any other data request or exercise of an individual's rights.

From time to time the College is required to share personal information with government and other agencies. Wherever possible, the College will make this clear in the Privacy Notices displayed or given at the point of collection. The College will ensure that data lawfully passed to government or other agencies is up to date and secure at the point of transfer, but after the transfer, the handling of the shared data will be subject to the terms of the recipient's privacy notices or privacy policy.

If there has been a data breach, this must be reported immediately to the member of staff's line manager and to the Data Protection Officer. Further details of the Breach Notification procedure are contained below.

Failure to comply with this policy, making or allowing an unlawful disclosure or any other breach of this data protection policy will be dealt with under the College's Disciplinary Policy.

## 19 Breach notification procedure

Whilst the College takes data security very seriously and has numerous policies and security measures in place to protect personal data, there is a possibility that, either due to human error or to external factors from third parties (eg hacking attack), a data breach could happen.

17.2 This breach may result in the unauthorised loss of, access to, deletion or alteration of personal data.

All College staff must report immediately any data breach, no matter how big or small, and whether or not a breach is likely to occur, is suspected of occurring or has actually occurred. On no account should staff try to resolve the breach directly, contact the individual(s) affected or take any other action themselves.

All College staff must report any breach/potential breach to both their line manager and the Data Protection Officer immediately it is known or suspected by telephone or by email.

The Data Protection Officer will then inform a member of the Executive Leadership Team and the College will then follow the Breach Notification procedure.

Immediate reporting of a suspected breach to the Data Protection Officer is essential to allow time for the College to assess, contain and manage the breach. Also, if the breach needs notifying to the Information Commissioners Office (ICO), this must be done within a maximum of 72 hours from becoming aware of the breach.

Once the breach procedure has been completed, the Data Protection Officer will record the breach and any evaluation on the College's data breach register.

Failure to report a data breach, attempting to resolve the matter directly or failure to follow this policy and the associated breach notification procedure will constitute grounds for action under the staff disciplinary policy.

Any issue or doubt over whether or not a breach has or has not occurred or over the notification procedure should be referred immediately to the Data Protection Officer (and in the Data Protection Officer's absence, to a member of the Executive Leadership Team).

## 20 Transfer of data outside the EEA/international transfers

Exports of data outside the European Economic Area (see definitions in **Appendix 1** for a list of EEA countries) are prohibited under the GDPR unless there is an appropriate level of data protection for the fundamental rights of the data subject.

The College will only transfer personal data outside the EEA if one or more of the specified safeguards or exceptions apply, namely:

- An assessment of adequacy has been made
- Privacy Shield framework has been adopted for US transfers
- Model contract clauses apply
- Binding corporate rules apply
- An exception applies

### Exceptions

In the absence of any of the above safeguards applying, transfers of data outside the EEA can only take place if at least one of the following exceptions exist:

- The individual has explicitly consented to the proposed transfer, having been informed of the possible risks of such transfers in the absence of appropriate safeguards.
- The transfer is necessary for the performance of a contract between the individual and the College or the implementation of pre-contract measures taken at the individual's request.
- The transfer is necessary for the conclusion or performance of a contract between the College and another natural or legal person which is in the interest of the individual.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the defence or exercising of legal claims by the College.

- The transfer is necessary in order to protect the vital interests of the individual or other persons, where the individual is physically or legally incapable of giving consent.

**Assessment of adequacy**

When making an assessment of adequacy, the College will take into account the following factors:

- The nature of the information being transferred.
- The country of origin and final destination of the information.
- How the information will be used and for how long.
- The laws and practices of the country the data is being sent to, including relevant codes of practice and international obligations.The security measures that are to be taken as regards the data in the overseas country

To ensure the College is compliant with these strict rules on international data, College staff must seek the immediate advice and authorisation of the Data Protection Officer before any data is exported from the UK.

## 21 Data Protection Impact Assessments (DPIAs)

The GDPR introduced a new requirement to carry out a risk assessment in relation to the use of personal data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment ("DPIA"). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using personal data but is an assessment of issues affecting personal data which need to be considered before a new product/service/process is rolled out.

The process is designed to:

- describe the collection and use of the personal data
- assess its necessity and its proportionality in relation to the purposes
- assess the risks to the rights and freedoms of individuals; and
- identify the measures to address the risks

Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College will consider whether it needs to carry out a DPIA as part of the project initiation process. The College will carry out a DPIA at an early stage in the process to identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

All College staff must complete a DPIA where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. Examples include the large scale processing of special category data such as health data or criminal convictions; also CCTV surveillance cameras.

College staff must use the DPIA form and must consult with the Data Protection Officer before and during the DPIA process.

Where, as a result of a DPIA it is clear that the College is about to start processing personal data which could cause damage and/or distress to the data subject, a decision will be made by a member of the Executive Leadership Team and the Data Protection Officer as to whether or not the College may proceed.

Where risks are identified in the DPIA, appropriate controls/actions will be selected and applied to reduce the level of risk associated with processing the data to an acceptable level to comply with the GDPR. The Data Protection Officer must then authorise any revised DPIA prior to any processing being started.

Staff must ensure all DPIAs are reviewed and approved by the Data Protection Officer.

The Data Protection Officer will keep a register of DPIAs in order to demonstrate compliance with GDPR principles.

## 22 Storage and Retention of Personal Data

Personal data (and sensitive personal data) will be stored securely in accordance with the College Information Security Policy.

Personal data (and sensitive personal data) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained. The information Asset Register sets out the relevant retention period, or the criteria that should be used to determine the retention period.

The agreed retention period for each type of information and the reasons for this are documented in the Group Information Asset Register, which provides a central record of all information processed by the Group.

When setting retention periods, consideration will be given to the following key factors:

- The purpose for which the data was obtained;
- Any specific consents provided by the data subject in relation to the use or retention of that data;
- Whether the original purpose has been fulfilled; and
- Whether the data needs to be retained to support any potential legal process.

Where there is any uncertainty with respect to data retention, staff should consult the Data Protection Officer.

The College has a legal responsibility not to keep personal data for longer than needed for the specific purposes agreed when it was collected. At the end of the agreed period for each type of information, also referred to as an Information Asset, managers will take steps to delete such information from its information systems, databases and electronic files and destroy paper records using agreed secure processes.

## 23 Training

Staff need to be adequately trained regarding their data protection responsibilities. Individuals whose roles required regular access to personal data, or who are responsible for implementing

this Policy or responding to subject access requests under this Policy, will receive additional training to them understand their duties and how to comply with them.

In addition to mandatory online training for all staff, face to face training sessions are held which introduce staff to the Data Protection Policy and to our procedures; including staff induction, College Management Team and department team meetings to enable ongoing dialogue around protecting personal data held by the College.

Business support staff with primary responsibility for the processing of personal and sensitive information receive training appropriate to their day to day duties and are required to maintain a level of operational understanding and awareness for the implementation of this policy and associated procedures. They will receive refresher training every year.

All staff receive a level of training appropriate to their role, with refresher training every 3 years. This will be recorded and monitored through central Workforce Development Records.

Students and other stakeholders will receive information and briefings appropriate to the personal data they provide, process or have access to, ensuring that all are aware of their rights and responsibilities with regard to data protection.

## 24 Policy review and maintenance

The Data Protection Officer is responsible for the maintenance, review and monitoring of the Data Protection Policy.

This policy shall be reviewed every 3 years and at other times as dictated by operational needs.

Copies of this policy and associated documentation are available from the College and the College website.

## Appendix 1: Definitions used in GDPR, Data Protection Policy and Privacy Notices

**Breach -** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There are reporting obligations to the supervisory authority (ICO) and where the breach is likely to adversely affect the personal data or privacy of the data subject.

**Child -** the GDPR 2018 defines a child as anyone under the age of 13 years old. The processing of personal data of a child is only lawful if parental consent has been obtained.

**College -** City College Plymouth.

**Consent -** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data.

**Controller -** any entity (e.g. company, organisation or person) which, alone or jointly with others, determines the purposes and the means of the processing of personal data. City College Plymouth is a data controller.

**Data -** any information relating to an identifiable person. The data can be processed either by computerised/automated systems or is recorded with the intention of using the information as such data. Data includes information kept by way of a relevant filing system e.g. paper/manual records.

**Data Protection Laws -** the General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

**Data subject -** any living individual who is the subject of personal data held by an organisation.

**DPIA (Data Protection Impact Assessment)** - this is a risk assessment of the data used by the College where a new product/service or process is introduced.

**Data Protection Officer (Data Protection Officer) -** the College has appointed a data protection officer who is the initial point of contact for all data protection issues and requests to exercise rights relating to data.

**EEA (European Economic Area) -** this includes Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

**Explicit consent -** consent obtained for the processing of specified personal data for a particular purpose.

**GDPR (General Data Protection Regulation (EU 2016/679) -** this is an EU regulation enacted in UK law as the Data Protection Act 2018.

**ICO (Information Commissioner's Office) -** the UK's data protection regulator.

**Individual -** a living individual who can be identified, directly or indirectly, from information that the College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

**Personal Data -** any information about an individual which identifies them or allows them to be identified. Personal data is defined broadly and covers things such as name, address, email address, IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

**Processing -** this term covers almost anything which is done with or to the data, including: collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Processor -** any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller.

City College Plymouth is a data processor.

A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains Personal Data, is provided by someone outside the organisation; cloud arrangements; and mail fulfilment services.

**Special Category Data -** Personal Data which reveals:

- A person's racial or ethnic origin
- Political opinions religious or philosophical beliefsTrade union membership
- Genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints)
- Physical or mental health
- Sexual life or sexual orientation

- Criminal offence/conviction records

Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

Special category data was previously known as “sensitive” data.

**Staff -** any College employee, worker or contractor who accesses any of the College’s Personal Data and will include employees, consultants, contractors, Governors, volunteers and temporary personnel hired to work on behalf of the College.

**Third party -** a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, authorised to process data.