Data Protection Policy

Reviewed: June 2018	**Next review due**: Currently under review
Approving Body: SLT	**SLT contact**: Chief Finance Officer
Policy approved by SLT: June 2018	

DATA PROTECTION POLICY

1 INTRODUCTION

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

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

1.3 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.

2 SCOPE

2.1 This policy applies to all members of College staff.

2.2 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

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

2.4 A Data Protection Officer (DPO) 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.

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

2.6 Staff and students will be made aware of the GDPR and this policy. They will be given guidance on complying with it and be informed of the consequences of failing to do so

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

2.8 This policy will be reviewed annually, though the College reserves the right to make changes to the policy and procedures at any time

2.9 All members of the Senior 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).

2.10 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.

3 OBJECTIVES

3.1 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.

3.2 This policy will demonstrate the College's application of its responsibilities under the GDPR 2018, in particular, the principles underpinning the GDPR.

3.3 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

3.4 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.

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

3.6 The policy will also refer to the Colleges retention policy for personal information

4 ASSOCIATED POLICIES AND DOCUMENTATION

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

- Documents annexed to this policy
- Information Security policy
- IT Security policy
- Computing and Digital Equipment Acceptable Use policy
- Social Media guidelines
- Home Working policy
- Bring Your Own Device (BOYD) policy
- Data retention policy

5 STAFF RESPONSIBILITIES

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

5.2 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.

5.3 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.

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

a) Outside the College;
b) Inside the College to College personnel not authorised to access the personal data

- without specific authorisation from the Data Protection Officer.

5.5 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.

5.6 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 DPO.

For more information on responding to data requests, refer to the Data Request Procedure at **Appendix 4**

5.7 Any data breach, breach of the GDPR or breach of this policy must be reported by staff to their manager and the Data Protection Officer as soon as possible. Staff must also follow the Data Breach Notification procedure set out in **Appendix 3** of this policy.

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

6 COLLEGE RESPONSIBILITIES

6.1 City College Plymouth is a data controller and a data processor under the GDPR 2018

6.2 Senior 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.

6.3 The Data Protection Officer and a member of the Senior Leadership Team is 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.

6.4 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.

6.5 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.

7 COLLEGE REGISTRATION WITH THE ICO

7.1 City College Plymouth is a data controller and processor under the GDPR 2018.

7.2 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.

7.3 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.

7.4 The College's current ICO registration number is Z4941564

7.5 Registration will be reviewed annually by the Data Protection Officer.

8 PUBLICATION OF COLLEGE INFORMATION

8.1 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 consent of a data subject.

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

8.3 It is the 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 e-mail addresses;
- Staff work contact numbers

8.4 The Senior 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.

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

8.6 Any individual who wishes details in these categories to remain confidential may contact the Chief Finance Officer to register their objection.

9 GDPR PRINCIPLES

9.1 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.

9.2 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 DPO if further clarification of any of these principles is required.

10 DEMONSTRATION OF COMPLIANCE WITH THE PRINCIPLES OF GDPR

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

10.2 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 (DPIA's) and by the appointment of a Data Protection Officer.

11 LAWFUL BASIS

11.1 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.

11.2 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

11.3 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

11.4 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.

11.5 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 these 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.

11.6 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

12 PRIVACY NOTICES AND TRANSPARENT PROCESSING

12.1 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.

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

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

12.4 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.

13 RIGHTS OF DATA SUBJECTS

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

13.2 The College ensures that individuals are made aware may exercise their rights

13.3 These rights are contained in the College's privacy notices and are also summarised below.

13.4 The procedure for dealing with a data request is contained in the Data Request procedure at **Appendix 4**

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 DPO.

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
legal@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 ,by telephoning 01752 305285 or by 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

14 DATA REQUESTS/ SUBJECT ACCESS REQUESTS

14.1 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 DPO what the request consists of, who has made the request and provide the DPO with a copy of the request

- Not make any attempt to deal with or respond to the request without authorisation from the DPO.

The DPO will then deal with the request, contact the individual and respond accordingly, following the Data Request procedure set out in **Appendix 4**.

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

15 DATA SECURITY

15.1 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.

15.2 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.

15.3 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

15.4 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 anonymization

- 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 (DPIA's) ,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.

16 **DISCLOSURE OF DATA BY STAFF**

16.1 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.

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

16.3 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

16.4 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

16.5 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 and at **Appendix 3**.

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

17 BREACH NOTIFICATION PROCEDURE

17.1 Whilst the College takes data security very seriously and has numerous policies and security measures 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.

17.3 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.

17.4 All College staff must report any breach/potential breach to both their line manager and the DPO Immediately it is known or suspected.

17.5 The Breach notification form at **Appendix 2** should be used to report the incident to the DPO. It provides a list of the details needed by the DPO to assess the breach initially. However, as time is of the essence, informing the DPO in person, by telephone or by email, is the main priority.

17.6 The DPO will then inform a member of the Senior Leadership Team and the College will then follow the Breach Notification procedure which is attached at **Appendix 3**.

17.7 Immediate reporting of a suspected breach to the DPO 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.

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

17.9 Failure to report a data breach, attempting to resolve the matter directly or failure to follow this policy and the associated breach notification procedure at

Appendix 3, will constitute grounds for action under the staff disciplinary policy.

17.10 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 DPO (and in the DPO's absence, to a member of SLT)

18 TRANSFERS OF DATA OUTSIDE THE EEA/ INTERNATIONAL TRANSFERS

18.1 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.

18.2 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

18.3 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 exists:

- 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 individuals 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.

18.4 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.

18.5 To ensure the College is compliant with these strict rules on international data, College staff must seek the immediate advice and authorisation of the DPO before any data is exported to a non –EEA country.

19 DATA PROTECTION IMPACT ASSESSMENTS (DPIA'S)

19.1 The GDPR introduces 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.

19.2 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 so that the College can 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.

19.3 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

19.4 College staff must use the DPIA form attached at **Appendix 5** and must consult with the DPO before and during the DPIA process.

19.5 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 Senior Leadership Team and the DPO as to whether or not the College may proceed.

19.6 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 DPO must then authorise any revised DPIA prior to any processing being started.

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

19.8 The DPO will keep a register of DPIA's in order to demonstrate compliance with GDPR principles.

20 POLICY REVIEW AND MAINTENANCE

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

20.2 This policy shall be reviewed annually and at other times as dictated by operational needs.

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

21 EQUALITY IMPACT ANALYSIS

21.1 Is this policy equality-relevant? If yes, list the groups of people who will be affected by this policy. **Yes. The policy affects all individuals equally**.

21.2 How have people from minority groups who may be affected by this policy been involved? **The policy applies equally to all individuals. No groups have been selected for consultation.**

21.3 What evidence has been considered? **Best practice drawn from the Information Commissioner's Office (ICO) website and also from the Association of Colleges (AoC)**

21.4 How does this policy fulfil the public sector duty by helping fight discrimination, advance equality of opportunity and foster good relations?

Equality Characteristic	How the Policy Helps Fulfil The Public Sector Duty
Age	**The policy implements UK data protection legislation which is age neutral for individuals over the age of 13**
Disability	**Consent to processing is subject to the individual being competent to give consent. If this is not the case, consent will be sought on the individual's behalf from a named guardian or next of kin.**
Gender identity	**Data protection legislation is gender neutral**
Ethnicity and race	**Sensitive data will be processed according to the requirements of the legislation**

Religion/belief	**Sensitive data will be processed according to the requirements of the legislation**
Sexual orientation	**Sensitive data will be processed according to the requirements of the legislation**
Pregnancy and maternity	**Sensitive data will be processed according to the requirements of the legislation**

21.5 Describe any potential adverse impacts that may arise as a result of this policy-
None

Appendix 1 Data Protection Policy

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 he or she, by a statement or by a clear affirmative action, signifies 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**.**

DPO (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 beliefs,

- Trade 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, are authorised to process data.

Appendix 2 Data Protection Policy

DATA BREACH NOTIFICATION FORM

TO BE COMPLETED AND PASSED TO DATA PROTECTION OFFICER IMMEDIATELY AFTER A DATA BREACH/POTENTIAL BREACH

Person who discovered breach: ……..…

Department: ……..……..

Person completing this form: …..……..

Department: …….

Time and date of breach: ……..……..

Nature of breach:

…….

……..…….

Description of breach:

…….

…….

…….

…….

…….

Personal data affected:

…….

…….

…….

Number of individuals affected/scale of breach: …….

Have any individuals affected contacted the College/complained? If so provide details:

…….

…….

Signed…….

Name ……. Date……

PLEASE ENSURE THIS FORM IS GIVEN IMMEDIATELY TO YOUR LINE MANAGER AND TO THE DATA PROTECTION OFFICER

APPENDIX 3 DATA PROTECTION POLICY

DATA BREACH NOTIFICATION PROCEDURE

This procedure forms part of the College's Data Protection policy.

Staff are referred to section 17 of that policy which sets out their obligations to report any potential or actual data breach to their manager and the DPO **immediately**.

This procedure is to be followed by all College staff where a data breach has occurred or is suspected of occurring, no matter how large or small the potential, suspected or actual breach.

1 WHAT IS A PERSONAL DATA BREACH?

A Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone does internally.

There are three main types of Personal Data breach which are as follows:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a member of College is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong party or not using "BCC" on emails, or disclosing information over the phone to the wrong person;

- **Availability breach -** where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

- **Integrity breach -** where there is an unauthorised or accidental alteration of Personal Data.

All College staff must report a data breach to their manager and the DPO immediately. The DPO and SLT will decide if the event constitutes a data breach- it is not for the member of staff concerned to decide whether the incident is defined as a breach or whether a breach has occurred.

College staff must not try and resolve matters directly themselves, contact the individual(s) affected or take any other action themselves other than reporting the incident to their manager and the DPO.

2 REPORTING A DATA BREACH

All College staff must report any breach or potential breach to their manager and the DPO immediately.

The data breach notification form attached at **Appendix 2** should be used to report the breach and should be sent to the DPO immediately on discovery of a breach. However, as time is of the essence, the main priority is to immediately inform the DPO, whether in person, by phone or by email of any suspected or actual breach.

The DPO will then inform a member of the Senior Management Team and the College will follow this breach notification policy.

Please refer to section 17 of the Data Protection policy for further instructions on how to report a breach.

Staff are reminded that failure to report a breach, trying to resolve an incident directly themselves or failure to follow the policy and notification procedure will constitute grounds for disciplinary action.

3 MANAGING A PERSONAL DATA BREACH

The College will identify and follow four elements in managing a Personal Data breach/potential breach:

- Containment and recovery
- Assessment of on-going risk
- Notification
- Evaluation and response

Containment and Recovery

An initial assessment of the Personal Data breach will be carried out by the Data Protection Officer.

If the Personal Data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected, then it will be added to the College's Data Breach Register and no further action will be taken.

If the Personal Data breach may impact on the rights and freedoms of the individuals affected, then the College will put together and implement a Personal Data breach plan to address the breach concerned in accordance with the College's Data Breach Notification Procedure. This will include consideration of:

- whether there are any other people within the College who should be informed of the breach, such as IT team members, to ensure that the breach is contained;

- -what steps can be taken to contain the breach, recover the loss of any Personal Data or to prevent damage being caused; and

- -whether it is necessary to contact other third parties such as students, parents, banks, the ICO or the police particularly in the case of stolen Personal Data. All notifications shall be made by the Data Protection Officer.

All actions taken in relation to a Personal Data breach will be in accordance with the Data Breach Notification Procedure which is maintained and administered by the Data Protection Officer.

The Data Protection Officer is responsible for ensuring that the Data Breach Register is updated.

Assessment of Ongoing Risk

As part of the College's response to a Personal Data breach, once the breach has been contained, the College will assess the on-going risks to the College and to any other party affected by the breach and what remedial action can be taken to minimise the impact of the breach. This will be undertaken in accordance with the College's Data Breach Notification Procedure.

Notification

Under Data Protection Laws, the College may have to notify the ICO and also possibly the individuals affected about the Personal Data breach.

Any notification will be made by the Data Protection Officer following the College's Data Breach Notification Procedure. The notification shall comply with the requirements of the ICO.

Notification of a Personal Data breach must be made to the ICO without undue delay and where feasible within 72 hours of when the College becomes aware of the breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. It is therefore imperative that College Personnel notify all Personal Data breaches to the College in accordance with the Data Breach Notification Procedure immediately.

Notification of a Personal Data breach must be made to the individuals affected without undue delay where the breach is likely to result in a high risk to the rights and freedoms of individuals.

Not all Personal Data breaches are notifiable to the ICO and/or the individuals affected and the College will decide whether to notify and who to notify in accordance with the Data Breach Notification Procedure.

Where the Personal Data breach relates to a temporary loss of availability of the College's systems, the College does not have to notify if the lack of availability of Personal Data is unlikely to result in a risk to the rights and freedoms of individuals. The College does not consider that it has any systems where temporary unavailability would cause a risk to the rights and freedoms of individuals but this will be assessed on a case-by-case basis in accordance with the Data Breach Notification Procedure.

In the case of complex breaches, the College may need to carry out in-depth investigations. In these circumstances, the College will notify the ICO with the information that it has within 72 hours of awareness and will notify additional information in phases. Any delay in notifying the ICO must be seen as exceptional and shall be authorised in accordance with the Data Breach Notification Procedure.

Where a Personal Data breach has been notified to the ICO, any changes in circumstances or any relevant additional information which is discovered in relation to the Personal Data breach shall also be notified to the ICO in accordance with the Data Breach Notification Procedure.

When the College notifies the affected individuals, it will do so in clear and plain language and in a transparent way. Any notifications to individuals affected will be done in accordance with the Data Breach Notification Procedure. Any notification to an individual should include details of the action the College has taken in relation to containing the breach and protecting the individual. It should also give any advice about what they can do to protect themselves from adverse consequences arising from the breach.

The College may not be required to notify the affected individuals in certain circumstances as exemptions may apply. Any decision whether to notify the individuals shall be done in accordance with the Data Breach Notification Procedure and shall be made by the Data Protection Officer.

Evaluation and Response

It is important not only to investigate the causes of the breach but to document the breach and evaluate the effectiveness of the College's response to it and the remedial action taken.

There will be an evaluation after any breach of the causes of the breach and the effectiveness of the College's response to it. All such investigations shall be carried out in accordance with the Data Breach Notification Procedure and will be recorded on the Data Breach Register kept by the DPO

Any remedial action such as changes to the College's systems, policies or procedures will be implemented in accordance with the Data Breach Notification Procedure.

APPENDIX 4 DATA PROTECTION POLICY

DATA REQUEST PROCEDURE

This procedure forms part of the Colleges Data Protection policy and is referred to in Section 14 of the policy.

This procedure sets out the steps to be followed when an individual exercises any of their data rights as set out in the GDPR.

It applies to all College staff who collect or use personal data relating to individuals.

It applies to all personal and special category data, whether the data is held electronically, on paper or otherwise.

If a member of staff receives a request from an individual to exercise any of their rights set out in the Data Protection policy and/or a Privacy notice, **the member of staff must**:

1. inform the Data Protection Officer (DPO) as soon as possible and in any event, within 24 hours of receiving the request

2. inform the DPO what the request consists of, who has made the request and provide the DPO with a copy of the request

3. not make any attempt to deal with or respond to the request without authorisation from the DPO.

The DPO will then deal with the request and follow the procedure below.

Individuals' rights include the right of access (often referred to as a "subject access request"), the right to rectification, the right to erasure (often referred to as the "right to be forgotten"), the right to restrict processing and the right to object to data being processed.

Please note some rights only apply in certain circumstances and are not automatic. For example, the right to object only applies where the lawful basis is for marketing purposes, performing tasks in the public interest or for legitimate interests. Also, the right to portability of data only applies where the lawful basis for processing is consent or performance of a contract.

College Data Request Procedure

1. On notification of the request, the DPO will assess each request, obtain clarification from the individual if needed, and make a decision as to whether the request is appropriate and/or consider any grounds for refusing the request.

2. Once the College is satisfied the request can be complied with, the College will begin locating the individual's data as soon as possible.

3. Depending on who the individual is, this may involve locating staff files, student files, information on parents, notes, minutes, emails, correspondence and other relevant documents containing personal data either on the College's information systems or in the College's structured paper filing systems. The DPO will advise College staff what searches they need to carry out.

4. Once the College has located all the personal data on the individual, the DPO will review it and decide whether any of the data does not need to be disclosed or exemptions apply

5. Once the College has decided what data is to be provided to the individual, the College will respond providing copies of the personal data which, if the request was made electronically, shall be provided in a commonly used electronic form.

   Copy information must be provided free of charge, except where it is deemed excessive when a reasonable fee can be charged based on the administrative costs of providing the information.

Response Times For Requests:

All requests by an individual to exercise their rights must be responded to and actioned within **one month** from the date the individual made the request. If the request is deemed by the DPO to be complex or there are multiple requests at once, the period may be extended up to a further 2 months. The College will notify the individual within the initial one month period if an extension is deemed necessary and the reasons for the extension.

Equally, if the College is not going to action the request by an individual, the DPO will inform the individual of this within one month from receipt of the request, giving reasons for refusing the request.

Refusals Of Requests

There are legitimate reasons under the GDPR where the College may refuse to action a request made by an individual and the College is allowed to retain or keep using the data. These reasons may relate to a request to for access/disclosure, the right to object or the right to erasure/to be forgotten. Reasons include:

- the fact that the data is needed for the assessment or
- collection of tax /duty, the information is publically available, or
- the information is covered by legal privilege or is needed to establish, exercise or defend legal rights and for evidential reasons.

In addition, if the College receives a request from an individual which is unfounded, excessive or repetitive, the College may either refuse to action the request, or charge a reasonable fee taking into consideration the College's administrative costs of providing the information or taking the action requested.

Any decisions in relation to not actioning a request or charging a fee will be made by the DPO and will be communicated to the individual within one month.

Informing Third Parties

Where an individual's right to rectification, erasure or restriction does apply, the College will as soon as possible contact any third parties who may have received the individual's information and inform the third party to correct, erase or restrict the data accordingly.

Right To Erasure/Right To Be Forgotten

Where an individual's right to erasure does apply, the College will first decide whether any parts of the data need to be retained/exempted for any legitimate reason. The College will then securely delete all the remaining personal data about the individual which is not exempt. This will include securely destroying all hard copy documents and ensuring that computer records are securely deleted from the College's information systems in line with the College's retention policy.

ANY QUERY OR REQUESTS BY INDIVIDUALS EXERCISING THEIR RIGHTS MUST BE REFERRED TO THE DPO IN THE FIRST INSTANCE.

DPIA No:

Appendix 5 -Data Protection Policy DATA PROTECTION IMPACT ASSESSMENT (DPIA)

This document is to be used to record a College DPIA process and outcome.

This DPIA document must not be started unless the College's Data Protection Officer has been previously informed.

Please refer to the College's Data Protection Policy for more information on DPIA's.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Appendix 5.docx

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for the College, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within the College? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA
Comments:		