Greater Brighton Metropolitan College

Privacy Standard

Policy review area	Governance
Lead Manager	Deputy COO/Director of MIS
Approval level	Board of Governors
Start date	April 2022
Review cycle	Yearly
Next review	April 2023

1. INTERPRETATION

1.1 **Definitions:**

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The Data Protection Legislation prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

College: Greater Brighton Metropolitan College.

College Personnel: all employees, workers, contractors, agency workers, consultants, officers, members and other staff of the College.

Consent: agreement, which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the Data Protection Legislation. We are the Controller of all Personal Data relating to our College Personnel and Personal Data used in our business for our own commercial purposes.

Criminal Convictions Data: Personal Data relating to criminal convictions and offences and includes Personal Data relating to criminal allegations and proceedings.

Data Protection Legislation: the UK Data Protection Legislation and /or, if the context so requires, any European Union legislation relating to personal data (including EU GDPR), and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programmes involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the Data Protection Legislation. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the College data privacy team with responsibility for data protection compliance.

EEA : the 27 countries in the EU, plus Iceland, Liechtenstein and Norway.

Explicit Consent: consent, which requires a very clear and specific statement (that is, not just action).

EU GDPR: the General Data Protection Regulation (*(EU) 2016/679*).

GDPR: the EU GDPR or UK GDPR, as the context requires.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Special Category Data, Criminal Convictions Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the Data Protection Legislation.

Privacy Guidelines: those privacy and Data Protection Legislation-related guidelines which the College may issue from time to time to assist in interpreting and implementing this Privacy Standard and Related Policies.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when the College collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or **Pseudonymised**: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the College's policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data, including but not limited to the Data Breach Policy.

Special Category Data: information falling within the meaning of “special categories of personal data”, as defined in the Data Protection Legislation, including information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

UK Data Protection Legislation: any data protection legislation from time to time in force in the UK including the Data Protection Act 2018 or any successor legislation and UK GDPR.

UK GDPR: as defined in the Data Protection Act 2018.

2. INTRODUCTION

This Privacy Standard sets out how we, the College, handle the Personal Data of our students, suppliers, employees, workers and other third parties.

This Privacy Standard applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, students, clients or supplier contacts, stakeholders, website users or any other Data Subject.

This Privacy Standard applies to all College Personnel ("you", "your"). You must read, understand and comply with this Privacy Standard when Processing Personal Data on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you in order for the College to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Privacy Standard. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Privacy Standard may result in disciplinary action.

Where you have a specific responsibility in connection with Processing such as capturing Consent, reporting a Personal Data Breach, conducting a DPIA as referenced in this Privacy Standard or otherwise then you must comply with the Related Policies and Privacy Guidelines.

This Privacy Standard (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

3. SCOPE

3.1 We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The College is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the Data Protection Legislation.

3.2 The Board of Governors is responsible for ensuring all College Personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure such compliance.

3.3 The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Shaun Mallin, Deputy COO and Director of MIS (email DPO@gbmc.ac.uk).

3.4 Please contact the DPO with any questions about the operation of this Privacy Standard or the Data Protection Legislation or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

3.4.1 if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the College) (see 5.1 below);

3.4.2 if you need to rely on Consent and/or need to capture Explicit Consent (see 5.2 below);

3.4.3 if you need to draft Privacy Notices (see 5.3 below);

3.4.4 if you are unsure about the retention period for the Personal Data being Processed (see 9 below);

3.4.5 if you are unsure about what security or other measures you need to implement to protect Personal Data (see 10 below);

3.4.6 if there has been a Personal Data Breach (see 10.6 and 10.7 below);

3.4.7 if you are unsure on what basis to transfer Personal Data outside the UK and/or the EEA (see 11 below);

3.4.8 if you need any assistance dealing with any rights invoked by a Data Subject (see 12 below);

3.4.9 whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see 13.5 below) or plan to use Personal Data for purposes others than what it was collected for;

3.4.10 if you need help complying with applicable law when carrying out direct marketing activities (see 13.6 below); or

3.4.11 if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see 13.7 below).

4. PERSONAL DATA PROTECTION PRINCIPLES

4.1 We adhere to the principles relating to Processing of Personal Data set out in the Data Protection Legislation which require Personal Data to be:

4.1.1 Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

4.1.2 Collected only for specified, explicit and legitimate purposes (Purpose Limitation);

4.1.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);

4.1.4 Accurate and where necessary kept up to date (Accuracy);

4.1.5 Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);

4.1.6 Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);

4.1.7 Not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

4.1.8 Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

5.1 **Lawfulness and fairness**
Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We will only process Personal Data for the specific purposes we identify as necessary and legitimate and as permitted by the Data Protection Legislation.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The Data Protection Legislation restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The Data Protection Legislation allows Processing for specific purposes, some of which are set out below:

5.1.1 the Data Subject has given his or her Consent;

5.1.2 the Processing is necessary for the performance of a contract with the Data Subject;

5.1.3 to meet our legal compliance obligations;

5.1.4 to protect the Data Subject's vital interests; and

5.1.5 to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

You must identify and document the legal ground being relied on for each Processing activity. If the legal ground being relied on has not been documented, then you must take steps to do so. If you are not certain of the appropriate legal ground, then you should raise this with your line manager.

5.2 **Consent**

A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the Data Protection Legislation, which includes Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Special Category Data or Criminal Convictions Data. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Special Category Data. Where Explicit Consent is required, you must issue a form of Privacy Notice to the Data Subject which includes provision for the Data Subject to give, or a consent form to capture, Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that the College can demonstrate compliance with Consent requirements.

5.3 **Transparency (notifying Data Subjects)**

The Data Protection Legislation requires Controllers to provide detailed, specific information to Data Subjects, depending on whether the information was collected directly from Data Subjects or from elsewhere. The information must be provided through appropriate Privacy

Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the Data Protection Legislation (including the identity of the Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data) through a Privacy Notice which must be presented when the Data Subject first provides the Personal Data.

Subject to limited exceptions, when Personal Data is collected indirectly (for example, from a third party or publicly available source), we must provide the Data Subject with all the information required by the Data Protection Legislation as soon as possible after collecting/receiving the data. We must also check that the Personal Data was collected by the third party in accordance with the Data Protection Legislation and on a basis which contemplates our proposed Processing of that Personal Data.

You will be provided with a Privacy Notice in respect of the information that has or will be collected about you, our reasons for Processing it and the legal bases for doing so.

6. PURPOSE LIMITATION

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for a different purpose from that disclosed when it was first obtained unless either (i) the new purpose is compatible with the original purpose (interpreted according to Article 6(4) of the GDPR); or (ii) you have informed the Data Subject of the new purposes and they have Consented where necessary.

7. DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

We will use appropriate technical and organisational measures to ensure that Personal Data that we no longer need is erased/destroyed. You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the College's data retention guidelines.

8. ACCURACY

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9. STORAGE LIMITATION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The College will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the College's Guidelines on Data Retention appended to this Privacy Standard.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the College's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

10. SECURITY INTEGRITY AND CONFIDENTIALITY

10.1 Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and field, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Category Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

10.1.1 *Confidentiality* means that only people who have a need to know and are authorised to use the Personal Data can access it;

10.1.2 *Integrity* means that Personal Data is accurate and suitable for the purpose for which it is processed; and

10.1.3 *Availability* means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the Data Protection Legislation and relevant standards to protect Personal Data.

10.2 **Safeguarding Personal Data**

Desks and cupboards should be kept locked if they hold Personal Data or confidential information of any kind. Data users must ensure that individual monitors/screens do not show Personal Data or confidential information to passers-by and that they log off from or lock their computer/tablet when it is left unattended.

10.3 Whenever we transfer Personal Data or confidential information outside our own systems or offices (for example when information is taken off site by employees to visit customers or for home working) there is a risk that the Personal Data or confidential information may be lost, misappropriated, or accidentally released.

10.4 Steps should be taken to minimise the risk of theft, loss, destruction, damage or unauthorised use of Personal Data or other confidential information when data is transferred. Such steps could include:

10.4.1 taking only the Personal Data that you need to take, ensuring that it is anonymised where possible and kept secure;

10.4.2 ensuring that bags or cases containing paper records are not left visible or unattended for longer than is absolutely necessary. If it is unavoidable to leave paper records in a vehicle (e.g. whilst refuelling) the data must be locked in a secure compartment or boot of the vehicle; and

10.4.3 ensuring that paper records are not carried 'loosely' but instead kept in a file or folder so that they are not visible to onlookers.

10.5 You should have permission from your manager before taking Personal Data off site. It must also be brought back and securely stored at the earliest opportunity.

10.6 **Personal Data Breaches**

10.6.1 The Data Protection Legislation requires Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

10.6.2 It is very important that we are alive to the risks of Personal Data Breaches, and that we react quickly to an apparent breach.

10.6.3 A Personal Data Breach may not be evident straightaway. However, there may be indicators of a Personal Data Breach, such as system compromise, unauthorised activity, or signs of misuse. A Personal Data Breach can happen in many ways, including:

(a) loss of a mobile device or hard copy file which contains Personal Data (e.g. leaving it on a train);

(b) theft of a mobile device or hard copy file which contains Personal Data (e.g. stolen from a vehicle or home);

(c) human error (e.g. a member of staff sending an email containing Personal Data to an unintended recipient, or accidentally altering or deleting Personal Data);

(d) cyber-attack (e.g. opening an attachment to an email from an unknown third party which contains ransomware or other malware);

(e) allowing unauthorised use/access (e.g. permitting an unauthorised third party to access secure areas of the office or our systems);

(f) unusual log-in and/or excessive system activity, in particular from any active user accounts;

(g) unusual remote access activity;

(h) the presence of any spoof wireless (Wi-Fi) networks visible or accessible from our working environment;

(i) accidental deletion of Personal Data;

(j) equipment failure;

(k) hardware or software key-loggers found connected to or installed on our systems;

(l) unforeseen circumstances such as a fire or flood; or

(m) 'blagging' offences where information is obtained from us by a third party through deception.

10.6.4 We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

10.7 **Reporting a Personal Data Breach**

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact your line manager and follow the Data Breach Plan. You should preserve all evidence relating to the potential Personal Data Breach.

11. TRANSFER LIMITATION

11.1 The Data Protection Legislation restricts data transfers to countries outside the UK and the EEA in order to ensure that the level of data protection afforded to individuals by the Data Protection Legislation is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

11.2 You may only transfer Personal Data outside the UK if one of the following conditions applies:

11.2.1 the transfer is to a country approved by the ICO in respect of Personal Data subject to UK GDPR (this is all Personal Data processed by the College), and the European Commission in respect of Personal Data subject to EU GDPR (for example, the Personal Data of EU students), as providing an adequate level of protection for the Data Subjects' rights and freedoms; or

11.2.2 appropriate safeguards are in place pursuant to Article 46, GDPR together with such supplementary measures as are necessary to bring the protection up to a level essentially equivalent to that guaranteed within the UK or the EU as the context requires, including (but not limited to) ensuring that the Personal Data is not shared with, or any access is allowed to such Personal Data, by any third party, Government agencies or other bodies, without the College's prior written consent, as well as ensuring any technical and security measures agreed between the College and transferee are complied with. Some examples of appropriate safeguards are:

(a) a legally binding agreement between public authorities or bodies;

(b) binding corporate rules (agreements governing transfers made between organisations within a corporate group);

(c) standard data protection clauses approved by the ICO (and in some cases the European Commission);

(d) compliance with an approved code of conduct approved by the Information Commissioner; and

(e) certification under an approved certification mechanism as provided for in the UK GDPR

11.3 Currently, it is possible to transfer Personal Data between the UK and the EEA without implementing any further safeguards. If you need to transfer Personal Data outside the EEA please speak to the Data Protection Officer to ensure that appropriate safeguards are put in place to authorise the transfer.

12. DATA SUBJECT'S RIGHTS AND REQUESTS

12.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

12.1.1 withdraw Consent to Processing at any time;

12.1.2 receive certain information about the Controller's Processing activities;

12.1.3 request access to their Personal Data that we hold;

12.1.4 prevent our use of their Personal Data for direct marketing purposes;

12.1.5 ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

12.1.6 restrict Processing in specific circumstances;

12.1.7 challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

12.1.8 request a copy of an agreement under which Personal Data is transferred outside of the UK and/or the EEA;

12.1.9 object to decisions based solely on Automated Processing, including profiling (ADM);

12.1.10 prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

12.1.11 be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

12.1.12 make a complaint to the relevant supervisory authority; and

12.1.13 in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

12.2 You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

12.3 You must immediately forward any Data Subject request you receive to your line manager and comply with the College's Response Procedures: Subject Access Requests process.

13. ACCOUNTABILITY

13.1 The Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Controller is

responsible for, and must be able to demonstrate, compliance with the data protection principles.

13.2 The College must have adequate resources and controls in place to ensure and to document Data Protection Legislation compliance including:

13.2.1 appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

13.2.2 implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

13.2.3 integrating data protection into internal documents including this Privacy Standard, Related Policies, Privacy Guidelines and Privacy Notices;

13.2.4 regularly training College Personnel on the Data Protection Legislation, this Privacy Standard, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The College must maintain a record of training attendance by College Personnel; and

13.2.5 regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

13.3 **Record keeping**

The Data Protection Legislation requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents [in accordance with the College's record keeping guidelines.]

These records should include, at a minimum, the name and contact details of the Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

13.4 **Training and audit**

We are required to ensure all College Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and, where applicable, ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

13.5 **Privacy by Design and Data Protection Impact Assessment (DPIA)**

We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Controllers must also conduct DPIAs in respect to high risk Processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

13.5.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

13.5.2 Automated Processing including profiling and Automated Decision-Making;

13.5.3 large scale Processing of Special Category Data; and

13.5.4 large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

13.5.5 a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

13.5.6 an assessment of the necessity and proportionality of the Processing in relation to its purpose;

13.5.7 an assessment of the risk to individuals; and

13.5.8 the risk mitigation measures in place and demonstration of compliance.

13.6 **Direct marketing**

We are subject to certain rules and privacy laws when marketing to our students or to potential students and their parents or legal guardians.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing students known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.
A Data Subject's objection to direct marketing must be promptly honoured. If a student opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

13.7 **Sharing Personal Data**

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding organisation along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

13.7.1 they have a need to know the information for the purposes of providing the contracted services;

13.7.2 sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

13.7.3 the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

13.7.4 the transfer complies with any applicable cross border transfer restrictions; and

13.7.5 a fully executed written contract that contains Data Protection Legislation approved third party clauses has been obtained.

13.8 **Information Sharing and Safeguarding Children and Young Adults**

We have a separate safeguarding policy and that must also be referred to when considering safeguarding issues relating to children and young adults.

UK Data Protection Legislation (in particular, the Data Protection Act 2018) allows for sharing of information without consent for the safeguarding of children and individuals at risk.

- Information can be shared legally without consent, if the College is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place a child at risk.

- Relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being.

Our DPO must be involved in any decision about data sharing for safeguarding reasons and we shall take the following principles into account before making such disclosure:

13.8.1 Necessary and proportionate

When taking decisions about what information to share, we must consider how much information we needs to release. Not sharing more data than is necessary to be of use is a key element of the Data Protection Legislation, and we should consider the impact of disclosing information on the data subject and any third parties. Information must be proportionate to the need and level of risk.

13.8.2 Relevant

Only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make informed decisions.

13.8.3 Adequate

Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

13.8.4 Accurate

Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

13.8.5 Timely

Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection to a child or young adult. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore place a child or young adult at increased risk of harm. We should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

13.8.6 Secure

Wherever possible, information should be shared in an appropriate, secure way. We must always follow our policy on security for handling personal information.

13.8.7 Record

We must record information sharing decisions, whether or not the decision is taken to share. If the decision is to share, we should cite the reasons including what information has been shared and with whom, in line with our organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and, if applicable, discuss them with the person who requested the information. In line with our data retention policy, the information should not be kept any longer than is necessary. In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so.

14. CHANGES TO THIS PRIVACY STANDARD

We reserve the right to change this Privacy Standard at any time without notice to you.

APPENDIX
GUIDELINES ON DATA RETENTION

1. INTRODUCTION

These guideline sets out the key issues that the College will consider when setting time limits for data retention and how data will be treated at the end of a retention period.

2. DATA STORAGE

Personal data may be stored in the following locations:

- our servers;
- third party servers;
- email accounts;
- desktops;
- employee-owned device (BYOD);
- backup storage; and/or
- paper files.

3. GENERAL RETENTION PERIODS

3.1. Generally, Personal Data should only be retained for as long as necessary to fulfil the purpose for which it was collected. The retention periods can differ based on the type of data processed, the purpose of processing or other factors. Issues to consider in determining long data should be retained include:

- Whether any legal requirements apply for the retention of any particular data. For example:
  - Trade law;
  - Tax law;
  - Employment law;
  - Administrative law; and
  - Regulations regarding the teaching profession.
- In the absence of any legal requirements, Personal Data may only be retained as long as necessary for the purpose of processing. This means data is to be deleted when:
  - the Data Subject has withdrawn consent to processing;
  - a contract has been performed or cannot be performed anymore; or
  - the data is no longer up to date.
- Has the Data Subject requested the erasure of data or the restriction of processing?
- Is the retention still necessary for the original purpose of processing?
- Exceptions may apply to the processing for historical, statistical or scientific purposes.

3.2. The College will establish and verify retention periods for data considering the following categories:

- requirements of the College;
- type of Personal Data;
- purpose of processing;
- lawful grounds for processing;
- lawful requirements for retention;
- litigation time limits; and
- types of Data Subjects

3.3. The established retention periods will either be set out in privacy notices given to Data Subjects or stated in a separate data retention policy.

3.4. The College will undertake periodical reviews of data it retains.

4. EXPIRATION OF THE RETENTION PERIOD

4.1. After the expiration of the applicable retention period Personal Data does not necessarily have to be completely erased. It is sufficient to anonymise the data. The College may achieve this by means of:

4.1.1. erasure of the unique identifiers which allow the allocation of a data set to a unique person;

4.1.2. erasure of single pieces of information that identify the Data Subject (whether alone or in combination with other pieces of information);

4.1.3. separation of Personal Data from non-identifying information (e.g. an order number from the individual's name and address); or

4.1.4. aggregation of Personal Data in a way that no allocation to any individual is possible.

4.2. In some cases, no action will be required if data cannot be allocated to an identifiable person at the end of the retention period, for example, because:

4.2.1. the pool of data has grown so much that personal identification is not possible based on the information retained; or

4.2.2. the identifying data has already been deleted.