DATA PROTECTION POLICY

February 2022

Endorsed by SMT:	2nd February 2022
Approved by F&GP:	8th March 2022
Next Evaluation/Review:	Spring 2023 and 2024 (SMT), Spring 2025 (SMT and F&GP)

1. INTRODUCTION

1.1. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College.

As an organisation that collects, uses and stores Personal Data about its students, parents, employees, governors, suppliers, visitors and volunteers, the College recognises that having controls around the collection, use, retention and destruction of Personal Data is important in order to comply with the College's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

The College has implemented this Data Protection Policy to ensure all College staff, including governors and volunteers, are aware of what they must do to ensure the correct and lawful treatment of Personal Data.

1.2. If you have any queries concerning this Policy, please contact a member of the Data Protection Team. The Data Protection Officer (DPO) role is split between 3 members of staff, the Principal, Deputy Principal and Director of Information Services:

- The Principal has overall responsibility for and is responsible for developing the College's Data Protection Policy and ensuring the College is compliant with legislation;
- The Deputy Principal is responsible for the delivery of the internal training to College staff;
- The Director of Information Services is responsible for providing technical expertise and guidance to the Principal and Deputy Principal and reporting data breaches to the ICO.

2. LEGISLATIVE FRAMEWORK

2.1. The following legislative framework informs the College's undertaking to protect the personal data of all stakeholders and comply with all legislative requirements.

- The General Data Protection Regulation 2018
- Data Protection Act 2018
- Information Commissioners Office (ICO): ICO Guide to Data Protection
- Freedom of Information Act 2000

3. SCOPE

3.1. The Data Protection Act 2018 regulates all activities that are involved with the "processing" of personal data. The definition of processing is very wide and therefore this policy assumes that everything that the college does with personal data is processing. Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- Organisation, adaptation or alteration of the information or data;
- Retrieval, consultation or use of the information or data;
- Disclosure of the information or data by transmission, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction of the information or data.

4. DEFINITIONS

4.1. Controller

A Controller is responsible for compliance with Data Protection Laws. The College will be viewed as a Controller of Personal Data as it decides what Personal Data we are going to collect and how we will use it. Individuals within organisations are not data controllers.

4.2. **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.

4.3. **Data Protection Officer**
The College's Data Protection Officer role is shared between three members of staff. See paragraph 1.2.

4.4. **EEA** – 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.

4.5. **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

4.6. **Individuals** – Living individuals 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.

4.7. **Personal Data** – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), 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.

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

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 business; cloud arrangements; and mail fulfilment services.

4.9. **Special Categories of Personal Data** – Personal Data that 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 and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

5. AIMS AND OBJECTIVES

5.1. The aim of this policy is to ensure that any processing of personal data complies with the Data Protection Act and GDPR. All processing of data should be compliant and in the spirit of all the data protection principles.

When using Personal Data, Data Protection Laws require that the College complies with the following principles. These principles require Personal Data to be:

5.1.1. processed lawfully, fairly and in a transparent manner;
5.1.2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
5.1.3. adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
5.1.4. accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
5.1.5. kept for no longer than is necessary for the purposes for which it is being processed; and
5.1.6. processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2. These principles are considered in more detail in the remainder of this Policy.

5.3. In addition to complying with the above requirements the College also has to demonstrate in writing that it complies with them. The College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the College can demonstrate its compliance.

6. LAWFUL USE OF PERSONAL DATA

6.1. In order to collect and/or use Personal Data lawfully the College needs to be able to show that its use meets one of a number of legal grounds. Please click here to see the detailed grounds https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing.

6.2. In addition when the College collects and/or uses Special Categories of Personal Data, the College has to show that one of a number of additional conditions is met. Please click here to see the detailed additional conditions https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data.

6.3. The College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 6.1 and 6.2. If the College changes how it uses Personal Data, the College needs to update this record and may also need to notify Individuals about the change. If College staff therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer team who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

7. TRANSPARENT PROCESSING – PRIVACY NOTICES

7.1. Where the College collects Personal Data directly from Individuals, the College will inform them about how the College uses their Personal Data. This is in a privacy notice. The College has a main Privacy Notice and separate Privacy Notices for Learner Enrolment and Governors and Trustees.

7.2. If the College receives Personal Data about an Individual from other sources, the College will provide the Individual with a privacy notice about how the College will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

7.3. If the College changes how it uses Personal Data, the College may need to notify Individuals about the change. If College staff therefore intend to change how they use Personal Data please notify the Data Protection Officer team who will decide whether the intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

8. DATA QUALITY – ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA

8.1. Data Protection Laws require that the College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the Individual in a privacy notice (see paragraph 7 above) and as set out in the College's record of how it uses Personal Data. The College is also required to ensure that the Personal Data the College holds is accurate and kept up to date.

8.2. Staff who collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

8.3. All staff who obtain Personal Data from sources outside the College shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require staff to independently check the Personal Data obtained.

8.4. In order to maintain the quality of Personal Data, all staff who access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

8.5. The College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws.

9. RETENTION OF DATA

9.1 The Act does not set out specific minimum or maximum periods for retaining personal data. It states personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. The college will keep some forms of information for longer than others. See Archiving Policy.

9.2 Due to storage considerations, information about students cannot be kept indefinitely, unless there are specific requests to do so. In general personal data relating to students will be kept for a minimum of seven years after the student's final course leaving date. This will include:

- Name and address;
- Academic achievements, including marks for coursework;
- Copies of any reference written; and
- The Learning Agreement.

9.3 The college will need to keep information about staff for a longer period. In general, all information will be kept for a minimum of seven years after a member of staff leaves the college. Some Human Resources information on the college database might be kept for longer. A full list of information with retention times is available from the Human Resources Manager.

10. DATA SECURITY

10.1. The College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

11. DATA BREACH

11.1 Whilst the College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and the College's Data Protection Officer team must be notified. Please see paragraphs 11.2 and 11.3 for examples of what can be a Personal Data breach.

11.2 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.

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

11.3.1 **Confidentiality breach** – where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a staff member 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 student, or disclosing information over the phone to the wrong person;

11.3.2 **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

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

12. APPOINTING CONTRACTORS WHO ACCESS THE COLLEGE'S PERSONAL DATA

12.1 If the College appoints a contractor who is a Processor of the College's Personal Data, Data Protection Laws require that the College only appoints them where the College has carried out sufficient due diligence and only where the College has appropriate contracts in place.

12.2 One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

12.3 Any contract where an organisation appoints a Processor must be in writing.

12.4 You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it they may get access to your Personal Data. Where you appoint a Processor you, as Controller remain responsible for what happens to the Personal Data.

12.5 GDPR requires the contract with a Processor to contain the following obligations as a minimum:

12.5.1 to only act on the written instructions of the Controller;
12.5.2 to not export Personal Data without the Controller's instruction;
12.5.3 to ensure staff are subject to confidentiality obligations;
12.5.4 to take appropriate security measures;
12.5.5 to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
12.5.6 to keep the Personal Data secure and assist the Controller to do so;
12.5.7 to assist with the notification of Data Breaches and Data Protection Impact Assessments;
12.5.8 to assist with subject access/individuals rights;
12.5.9 to delete/return all Personal Data as requested at the end of the contract;
12.5.10 to submit to audits and provide information about the processing; and
12.5.11 to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

12.6 In addition the contract should set out:

12.6.1 the subject-matter and duration of the processing;
12.6.2 the nature and purpose of the processing;
12.6.3 the type of Personal Data and categories of individuals; and
12.6.4 the obligations and rights of the Controller.

13. INDIVIDUALS' RIGHTS

13.1 GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced. It is extremely important that Colleges plan how they will handle these requests under GDPR.

13.2 The different types of rights of individuals are reflected in this paragraph.

13.3 Subject Access Requests

13.3.1 Individuals have the right under the GDPR to ask a College to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right but additional information has to be provided and the timescale for providing it has been reduced from 40 days to one month (with a possible extension if it is a complex request). The College is not able to charge a fee for complying with the request.
13.3.2 Subject Access Requests are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

13.4 Right of Erasure (Right to be Forgotten)

13.4.1 This is a limited right for individuals to request the erasure of Personal Data concerning them where:

13.4.1.1 the use of the Personal Data is no longer necessary;
13.4.1.2 their consent is withdrawn and there is no other legal ground for the processing;
13.4.1.3 the individual objects to the processing and there are no overriding legitimate grounds for the processing;
13.4.1.4 the Personal Data has been unlawfully processed; and
13.4.1.5 the Personal Data has to be erased for compliance with a legal obligation.

13.4.2 In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

13.5 **Right of Data Portability**

13.5.1 An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine readable format where:

13.5.1.1 the processing is based on consent or on a contract; and
13.5.1.2 the processing is carried out by automated means.

13.5.2 This right isn't the same as subject access and is intended to give individuals a subset of their data.

13.6 **The Right of Rectification and Restriction**

13.6.1 Finally, individuals are also given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

13.7 The College will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Laws, and will ensure that it allows Individuals to exercise their rights.

14. AUTOMATED DECISION MAKING AND PROFILING

14.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

14.1.1 **Automated Decision Making** happens where the College makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and
14.1.2 **Profiling** happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

14.2 Any Automated Decision Making or Profiling which the College carries out can only be done once the College is confident that it is complying with Data Protection Laws. If College staff therefore wish to carry out any Automated Decision Making or Profiling College staff must inform the Data Protection Officer team.

14.3 College Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer team.

14.4 The College does not carry out Automated Decision Making or Profiling in relation to its employees.

15. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

15.1 The GDPR introduce 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:

15.1.1 describe the collection and use of Personal Data;
15.1.2 assess its necessity and its proportionality in relation to the purposes;
15.1.3 assess the risks to the rights and freedoms of individuals; and
15.1.4 the measures to address the risks.

15.2 A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The ICO's standard DPIA template is available from www.ico.org.uk.

15.3 Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

15.4 Where the College is launching or proposing to adopt a new process, product or service which involves Personal Data, the College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The College needs to 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.

15.5 Situations where the College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

15.5.1 large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;
15.5.2 large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or
15.5.3 systematic monitoring of public areas on a large scale e.g. CCTV cameras.

15.6 All DPIAs must be reviewed and approved by the Data Protection Officer team.

16. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

16.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA.

16.2 So that the College can ensure it is compliant with Data Protection Laws College staff must not export Personal Data unless it has been approved by the Data Protection Officer team.

16.3 College staff must not export any Personal Data outside the EEA without the approval of the Data Protection Officer team.

17. RESPONSIBILITIES: STAFF

17.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the college. Any failures to follow the policy may result in disciplinary proceedings.

17.2 A member of staff, who considers the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated DPC initially. If the matter is not resolved it should be raised as a formal grievance.

17.3 All staff are responsible for:

17.3.1 checking that any information that they provide to the college in connection with their employment is accurate and up-to-date;
17.3.2 informing the college of any changes to information, which they have provided, for example changes of address;
17.3.3 checking the information that the college will send out from time to time, giving details of information kept and processed about staff; and
17.3.4 informing the college of any errors or changes to personal data. The college cannot be held responsible for any errors unless the staff member has informed the college of them.

17.4 If and when, as part of their responsibilities, staff collect information about other people, (e.g. about students' coursework, opinions about ability, reference to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff on SharePoint.

17.4.1 any personal data which a member of staff holds must be kept safe and only used for legitimate purposes (see Fair Notice);
17.4.2 personal data must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party;
17.4.3 sensitive data should be: Kept in a locked filing cabinet, drawer, office or if it is computerised, be password protected or if staff access sensitive data on a personal device it should be password or PIN protected (e.g. E-mail linked to their smartphone); and
17.4.4 no sensitive data should be kept only on disk, usb drive or tablet.

17.5 Compliance with the Data Protection Act 2018 is the responsibility of all members of the college. Any deliberate breach (including non-disclosure of data loss, paper, phone or tablet) of the Data Protection Policy may lead to disciplinary action being taken, or access to college facilities being withdrawn, or even a criminal prosecution. Staff should also note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

17.6 Any questions or concerns about the interpretation or operation of this Policy should be taken up with the designated Data Controllers.

18. RESPONSIBILITIES: STUDENTS

18.1 Students must ensure that all personal data provided to the college is accurate and up-to-date. They must ensure that changes of personal details are notified to their tutor who in turn will inform the Registry team.

18.2 Students who use the college computer facilities may, from time to time, process personal data which will be password protected. Access to some student personal data can be viewed via the students' "MyProgress" interface.

19. MONITORING

19.1 Rights to access information:

19.1.1 Staff, students and other users of the college have the right to access any personal data that is being kept about them either on computer or other format. Any person who wishes to exercise this right should complete the college 'Access to Information' form and give it to Reception;
19.1.2 The college aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one calendar month unless there is a good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request; and
19.1.3 Information that is already in the public domain is exempt from the Data Protection Policy and is covered by the college's Publication Scheme.

19.2 Subject Consent:

19.2.1 In many cases, the college can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the college processing some specified classes of personal data is a condition of acceptance of a student onto any course, and a condition of employment for staff. This includes information about previous criminal convictions;

19.2.2 Some jobs or courses will bring the applicants into contact with children, including young people between the ages of 16 and 18. The college has a duty under the Children Act and other enactments to ensure that staff are suitable for the job, and students for the courses offered. The college also has a duty of care to all staff and students and must, therefore, make sure that employees and those who use the college facilities do not pose a threat or danger to other users. Where an enhanced Disclosure and Barring check is required consent will be requested and information collected, stored and processed in accordance with the Data Protection Act 2018. A refusal to sign such a form can result in the offer of a position, paid or voluntary (staff including governors and volunteers) or course (students) being withdrawn;

19.2.3 The college will also ask for information about particular health needs, such as allergies to particular forms of medication, or any conditions such as asthma or diabetes. The college will only use the information in the protection of the health and safety of the individual, but will need consent to process for example in the event of a medical emergency;

19.2.4 Therefore, all prospective staff (including volunteers and governors) and students will be asked to sign a '*Consent to Process'* form, regarding particular types of information when an offer of a position or a course place is made; and

19.2.5 Prospective staff (including volunteers and governors) will be asked to sign an HR data form to give permission for specified personal data to be shared with authorised staff. The staff employment contract gives specific consent to the college retaining computer and paper based records.

20. PROCESSING SENSITIVE INFORMATION

20.1 Occasionally it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure that the college is a safe place for everyone, or to operate other college policies, such as the Equality and Diversity Policy. As this information is considered sensitive and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and students will be asked to give express consent for the college to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the Human Resources Manager or Student Services.

21. CCTV AND BODY WORN CAMERAS (BWC) CODE OF PRACTICE

21.1 The CCTV and Body Worn Cameras Code of Practice is to regulate the management, operation and use of the CCTV and Body Worn Cameras at the College and is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and will seek to comply with the requirements of the Data Protection Act, the Commissioner's Code of Practice and the Freedom of Information Act 2000.

22. EXAMINATION MARKS

22.1 Students will be entitled to information about their examination marks. However, this may take longer than other information to provide. The college may withhold certificates or references in the event that the full course fee has not been paid (when applicable), there are outstanding debts or books, equipment or materials have not been returned to the college.

23. **SECURITY**

23.1 The college will take all appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

RELATED POLICIES and PROCEDURES

Appeals Procedure Staff
Appeals Procedure Non-Staff
CCTV and Body Worn Cameras (BWC) Code of Practice
Copyright Policy
Equality and Diversity Policy
Health and Safety Policy
Learner Enrolment Privacy Statement
Privacy Notice (How we use your Personal Data)
Safeguarding Policy
Social Media Policy
Staff Code of Conduct
Staff Disciplinary Policy
Student Code of Conduct
Student Disciplinary Policy
The Publication Scheme
Use of Computers Agreement