General Data Protection Policy 2024-27

Author:	Executive Director Digital Transformation and Planning
Policy Date:	October 2024
Review Date:	June 2027
Procedure available:	Intranet and Website
Authorised by:	Executive and Corporation

TABLE OF CONTENTS

1. OVERVIEW

The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the College.

Buckinghamshire College Group is an organisation that collects, uses and stores Personal Data about its employees, suppliers (sole traders, partnerships or individuals within companies), students, alumni, governors, parents and visitors. 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 Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in the College and will provide for a successful working and learning environment for all.

College Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any member of the College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All members of College Personnel are obliged to comply with this Policy at all times.

If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the College's compliance with this Policy.

2. ABOUT THIS POLICY

This Policy (and the other policies and documents referred to in it) sets out the basis on which the College will collect and use Personal Data either where the College collects it from individuals itself, or where it is provided to the College by third parties. It also sets out rules on how the College handles uses, transfers and stores Personal Data.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

3. DEFINITIONS

3.1. **College** – Buckinghamshire College Group

3.2. **College Personnel** – Any College employee, worker or contractor who accesses any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College. This also includes governors.

3.3. **Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.

A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data the College is the Controller of include employee details or information the College collects relating to students. The College will be viewed as a Controller of Personal Data if it decides what Personal Data the College is going to collect and how it will use it.

A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.

3.4. **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.

3.5. **Data Protection Officer –** Our Data Protection Officer is the Executive Director MIS and Digital Transformation, and can be contacted at: foi@buckscollegegroup.ac.uk

3.6. **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.

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

3.8. **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.

3.9. **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.

3.10. **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.

3.11. **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.

4. COLLEGE PERSONNEL'S GENERAL OBLIGATIONS

4.1. All College Personnel must comply with this policy.

4.2. College Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

4.3. College Personnel must not release or disclose any Personal Data:

4.3.1. outside the College; or

4.3.2. inside the college to College Personnel not authorised to access the Personal Data, without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

4.4. College Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other College Personnel who are not authorised to see such Personal Data or by people outside the College.

5. DATA PROTECTION PRINCIPLES

5.1. 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 special categories of personal data | Search | Information Commissioner's Office

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 0. 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 Personnel therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer 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 privacy notices are included in Appendix 1 and available via the College website.

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 Personnel therefore intend to change how they use Personal Data please notify the Data Protection Officer who will decide whether the College Personnel's 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. All College Personnel that 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 College Personnel that 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 College Personnel to independently check the Personal Data obtained.

8.4. In order to maintain the quality of Personal Data, all College Personnel that 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. The College has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the College responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

9. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED

9.1. Data Protection Laws require that the College does not keep Personal Data longer than is necessary for the purpose or purposes for which the College collected it.

9.2. The College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed by the

College, the reasons for those retention periods and how the College securely deletes Personal Data at the end of those periods.

9.3. If College Personnel feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Data Retention Policy, for example because there is a requirement of law, or if College Personnel have any questions about this Policy or the College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

10. DATA SECURITY

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 College Personnel must comply with the College's Data Breach Notification Policy. Please see paragraphs 11.2 and 11.3 for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which College Personnel need to comply with in the event of Personal Data breaches.

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. 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 internal does.

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 College Personnel 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). In addition, you will no longer be able to charge a fee for complying with the request.

13.3.2. Subject Access Requests are becoming more and more common and 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 in accordance with the College's Rights of Individuals Policy and Rights of Individuals Procedure.

Please familiarise yourself with these documents as they contain important obligations which College Personnel need to comply with in relation to the rights of Individuals over their Personal Data.

14. MARKETING AND CONSENT

14.1. The College will sometimes contact Individuals to send them marketing or to promote the College. Where the College carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

14.2. Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR will bring about a number of important changes for organisations that market to individuals, including:

14.2.1. providing more detail in their privacy notices, including for example whether profiling takes place; and

14.2.2. rules on obtaining consent will be stricter and will require an individual's "clear affirmative action". The ICO like consent to be used in a marketing context.

14.3. Colleges also need to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. PECR apply to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data

14.4. Consent is central to electronic marketing. We would recommend that best practice is to provide an un-ticked opt-in box.

14.5. Alternatively, the College may be able to market using a “soft opt in” if the following conditions were met:

14.5.1. contact details have been obtained in the course of a sale (or negotiations for a sale);

14.5.2. the College are marketing its own similar services; and

14.5.3. the College gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

15. AUTOMATED DECISION MAKING AND PROFILING

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

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

Profiling happens where the College automatically uses Personal Data to evaluate certain things about an Individual.

15.2. 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 Personnel therefore wish to carry out any Automated Decision Making or Profiling College Personnel must inform the Data Protection Officer.

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

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

16. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

16.1. 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:

16.1.1. describe the collection and use of Personal Data;

16.1.2. assess its necessity and its proportionality in relation to the purposes;

16.1.3. assess the risks to the rights and freedoms of individuals; and

16.1.4. the measures to address the risks.

16.2. 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.

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

16.4. 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.

16.5. 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):

16.5.1. 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;

16.5.2. 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

16.5.3. systematic monitoring of public areas on a large scale e.g. CCTV cameras.

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

17. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

17.1. 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. It needs to be thought about whenever the College appoints a supplier outside the EEA or the College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

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

17.3. College Personnel must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

Appendix 1 – Privacy Notices

Staff Privacy Notice

How we use workforce information
Under data protection law, individuals have a right to be informed about how Buckinghamshire College Group uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use your personal data and data about you. We, Buckinghamshire College Group are the 'data controller' for the purposes of data protection law. Our data protection officer is Rachael Murray, Executive Director MIS and Planning.
The categories of workforce information that we collect, process, hold and share include:

- your name, address and contact details, including email address and telephone number, date of birth and gender
- the terms and conditions of your employment
- details of your qualifications, skills, experience and employment history, including start and end dates, with previous employers and with the organisation
- information about your remuneration, including entitlement to benefits such as pensions or insurance cover
- details of your bank account and national insurance number
- information about your marital status, next of kin, dependants and emergency contacts
- information about your nationality and entitlement to work in the UK
- information about your criminal record
- details of your schedule (days of work and working hours) and attendance at work
- details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals, and the reasons for the leave
- details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence
- assessments of your performance, including appraisals, performance reviews and ratings, training you have participated in, performance improvement plans and related correspondence
- information about medical or health conditions, including whether or not you have a disability for which the organisation needs to make reasonable adjustments
- details of trade union membership
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief

Why we collect and use this information
The College needs to process data to enter into an employment contract with you and to meet its obligations under your employment contract. For example, it needs to process your data to provide you with an employment contract, to pay you in accordance with your employment contract and to administer benefit, pension and insurance entitlements.

In some cases, the College needs to process data to ensure that it is complying with its legal obligations. For example, it is required to check an employee's entitlement to work in the UK, to deduct tax, to comply with health and safety laws and to enable employees to take periods of leave to which they are entitled. For all positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to work within the College.

In other cases, the College has a legitimate interest in processing personal data before, during and after the end of the employment relationship. Processing employee data allows the College to:

- Run recruitment and promotion processes
- Maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights
- Operate and keep a record of disciplinary, grievance, safeguarding and capability processes, to ensure acceptable conduct within the workplace
- Operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes
- Operate and keep a record of absence and absence management procedures, to allow effective workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled
- Obtain occupational health advice, to ensure that it complies with duties in relation to individuals with disabilities, meet its obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled
- Operate and keep a record of other types of leave (including maternity, paternity, adoption, parental and shared parental leave), to allow effective workforce management, to ensure that the organisation complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled
- Ensure effective general HR and business administration, this includes using the data to help test the HR system as appropriate
- Provide references on request for current or former employees
- Respond to and defend against legal claims
- Maintain and promote equality in the workplace

Where the College relies on legitimate interests as a reason for processing data, it has considered whether or not those interests are overridden by the rights and freedoms of employees or workers and has concluded that they are not.

Some special categories of personal data, such as information about health or medical conditions, is processed to carry out employment law obligations (such as those in relation to employees with disabilities and for health and safety purposes).

Where the College processes other special categories of personal data, such as information about ethnic origin, sexual orientation, health or religion or belief, this is done for the purposes of equal opportunities monitoring. Data that the organisation uses for these purposes is anonymised or is collected with the express consent of employees, which can be withdrawn at any time. Employees are entirely free to decide whether or not to provide such data and there are no consequences of failing to do so.

The lawful basis on which we process this information

You have some obligations under your employment contract to provide the College with data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide the College with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable the College to enter a contract of employment with you. If you do not provide other information, this will hinder the College's ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

The lawful basis on which we process workforce information under Article 6 of GDPR is as follows:

“(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;”
and/or
“(c) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;”
Where data processed is classified as special category data under GDPR, the lawful basis on which we process workforce information under Article 9 of GDPR is as follows:
“(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;”

We only collect and use workforce personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Less commonly, we may also process workforce personal data in situations where:

- We have obtained consent to use it in a certain way
- We need to protect the individual’s vital interests (or someone else’s interests)

Where we have obtained consent to use workforce personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Some of the reasons listed above for collecting and using workforce personal data overlap, and there may be several grounds which justify our use of this data.

Collecting this information

The College collects this information in a variety of ways. For example, data is collected through application forms, CVs or resumes; obtained from your passport or other identity documents such as your driving licence; from forms completed by you at the start of or during employment; from correspondence with you; or through interviews, meetings or other assessments.

In some cases, the College collects personal data about you from third parties, such as references supplied by former employers, information from criminal records checks permitted by law and information divulged from the Council’s Safeguarding Children’s and Adults Boards in relation to safeguarding allegations

Data is stored in a range of different places, including in your personnel file, in the College's HR management system (iTrent) and in other IT systems (including the College's email system and the IT storage drives).

Storing this information

The College takes the security of your data seriously. The College has internal policies and controls in place to try to ensure that your data is not lost, accidentally destroyed, misused or disclosed, and is not accessed except by its employees in the performance of their duties.

Where the College engages third parties to process personal data on its behalf, they do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

The College will hold your personal data for the duration of your employment. Your data is held for 7 years after the end of your employment except for pension and safeguarding information which is retained indefinitely. At the end of that period (or once you withdraw your consent), your data is deleted or destroyed.

When data is stored and/or retained, we will continually:

- review the length of time we keep personal data;
- consider the purpose or purposes that we hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes;
- update, archive or securely delete information if it goes out of date or is no longer required

Who we share this information with

Your information will be shared internally, including with members of the HR team, the finance department, your line manager and IT staff if access to the data is necessary for performance of their roles. Should a grievance or disciplinary investigation be required, relevant information to that investigation may be shared upon approval by the Executive Director Human Resources.

The College shares your data with third parties in order to obtain references from other employers and obtain necessary criminal records checks from the Disclosure and Barring Service. The College may also share your data with third parties in the context of a sale of some or all of its business. In those circumstances the data will be subject to confidentiality arrangements.

The College also shares your data with third parties that process data on its behalf, in connection with payroll, pension scheme providers, the provision of benefits and the provision of occupational health services.

We will only share your information with partners or suppliers who have sufficient measures and procedures in place to protect your information and can meet their legal obligations under data protection legislation.

Why we share workforce information

We do not share information about workforce members with anyone without consent unless the law and our policies allow us to do so.

Data collection requirements

JOB APPLICANTS, CURRENT EMPLOYEES AND FORMER EMPLOYEES

How we use your information

The information we ask for is used to assess your suitability for employment. You don’t have to provide what we ask for but it might affect your application if you don’t.

Application stage

We ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, referees and for answers to questions relevant to the role you have applied for.

Our recruitment team will have access to all of this information.

You will also be asked to provide equal opportunities information. This is not mandatory information – if you don’t provide it, it will not affect your application. This information will not be made available to any staff outside of our recruitment team, including hiring managers, in a way which can identify you. Any information you do provide will be used only to produce and monitor equal opportunities statistics.

Shortlisting

Our hiring manager's shortlist applications for interview. They will not be provided with your name or contact details or with your equal opportunities information if you have provided it.
Candidates are asked to provide proof of identity and qualifications at the interview. Photocopies of original documents are only retained if the candidate is successful.

If you are unsuccessful for the position you have applied for, your data will be held for a period of six months in case of any queries regarding the outcome or for feedback purposes.

Conditional offer

If we make a conditional offer of employment, we will ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We are required to confirm the identity of our staff, their right to work in the United Kingdom and assess suitability for the role.

Upon commencement of your employment, we will also ask you for:

Bank details – to process salary payments
Emergency contact details – so we know who to contact in case you have an emergency at work
Employment status for tax code purposes.

Our contract of employment requires all staff to declare if they have any potential conflicts of interest, other employment or engagement. If you complete a declaration, the information will be held on your personnel file.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Isobel Ellison, Executive Director Human Resources or Rachael Murray, Data Protection Officer.

You also have the right to:

- access and obtain a copy of your data on request;
- require the College to change incorrect or incomplete data;
- require the College to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing;
- object to the processing of your data where the College is relying on its legitimate interests as the legal ground for processing; and
- ask the College to stop processing data for a period if data is inaccurate or there is a dispute about whether or not your interests override the College's legitimate grounds for processing data or claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information
If you would like to discuss anything in this privacy notice, please contact: Executive Director MIS and Digital Transformation & Data Protection Officer

Student Privacy Notice

How we use student information

We, Buckinghamshire College Group (the **College**), collect personal information about yourself in order for you to apply and enrol as a student and to allow you to use College systems and services.

Primarily, your personal data may be used for: -

- Administrative services, such as course registration, examination, and certification.
- The provision of student support services and other student guidance.
- Statistical, funding and research purposes, relating to education, training, employment and well-being.

When we do collect your personal data, we are regulated under the General Data Protection Regulation (**GDPR**) which applies across the European Union (including in the United Kingdom) and we are responsible as 'controller' of that personal information for the purposes of those laws.

This privacy notice was last updated October 2024.

The categories of student information that we collect, hold and share include:

- **Identity and Contact Data**: personal information (such as name, date of birth, next of kin details, unique learner number, national insurance number, home address, email address and telephone number).
- **Characteristics Data**: gender, ethnicity, nationality, country of birth, country of domicile).
- **Disabilities Data**: Disclosed and assessed learning difficulties / disabilities.
- **Historical Data**: Prior attainment levels and the details of previous educational institutions attended.
- **Employment Data:** Current employment status
- **Criminal Data**: Criminal convictions and offences.
- **Attendance Data:** Attendance information (such as sessions attended, number of absences and absence reasons)
- **Study Data**: Study programme details.
- **Assessment Data:** grades awarded, modules completed, qualifications completed.
- **Image Data:** Photographic images or video footage (only where we have obtained explicit consent), CCTV footage.
- **Destination** Data: destination and progression records (such as name of institution/organisation that a student attends upon leaving the College).

Why we collect and use this information

We use your personal data:

- to support student learning and achievement
- to track, monitor and report on student progress
- to provide appropriate pastoral care
- to ensure the health, safety and wellbeing of students
- to assess the quality of our services
- to meet statutory funding arrangements
- to comply with the law regarding data sharing

The lawful basis on which we use this information

We will process your personal data for one or more of the following lawful grounds:

- Where we need to perform the contract we are about to enter into or have entered into with you.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.
- Where it is in your vital interest in order to keep you safe – for example, CCTV footage.
- Where we need to comply with a legal or regulatory obligation.
- Where we need to in order to protect your health and well-being or the health and well-being of someone else – for example, other students.
- Where we rely on your consent – for example, where you agree we can send you information about our other courses.

We call the above grounds **Fundamental Grounds** in the rest of this section.

When we process certain types of data called “special categories of personal data” (which may include, for example, Characteristics Data, Disabilities Data, Historical Data, Attendance Data and Assessment Data), we will process these special categories of personal data on one or more of the Fundamental Grounds together with one or more of the following lawful grounds;

- Where we have obtained your explicit consent;
- Where we need to assess your capacity to study.
- Where we need to collect these types of information for statistical purposes.
- Where we need to in order to protect your health and well-being or the health and well-being of someone else – for example, other students – and you cannot give your consent, or we cannot be expected to obtain your consent, or where you have unreasonably withdrawn your consent.
- Where we need to collect and use information about your race or ethnicity to identify or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and, where we do so. we will put in place appropriate safeguards for your rights and freedoms.

When we process Criminal Data, we will process this data for one or more of the Fundamental Grounds and because we are authorised to do so under the laws of the United Kingdom or because we are doing it under the control of an official authority.

Please contact us if you need details about the specific legal ground we are relying on to process your personal data.

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

Storing student data

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your

personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

For European Union (EU) funded projects, we are required to keep records until 31st December 2025.

Who we share student information with

We routinely share student information with:

- educational institutions that the student attends after leaving the College
- educational institutions that the student has attended before joining the College
- Local Authorities
- the Department for Education (DfE)
- the Education and Skills Funding (ESFA)
- the Office for Students (OfS)
- the Learner Records Service (LRS)
- the National Careers Service
- any other Government Agency where we are required to share your data
- those organisations awarding the qualifications that we offer
- parents / carers / guardians
- employers that sponsor a student on a course of study
- Agencies who are required to audit our student and financial records
- Agencies who support the collection of unpaid / outstanding course fees

We will not share your personal information with any other third party.

Why we share student information

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

We have found that academic success is closely linked to the involvement and support of parents, guardians and carers. For this reason, the College will share information in respect of academic progress and attendance with parents, carers and guardians of students below 18 years of age who have been named at enrolment at the College. For students aged below 18 at the start of their programme, but who turn 18 during the academic year, we will continue to share information with parents, carers and guardians for the duration of the academic year. For those aged 18 or over at the start of an academic year, information will only be shared where prior consent has been obtained. Likewise, we also have a policy of sharing the same information with employers that sponsor a student on a programme of study.

We share student data with the DfE, ESFA, OfS and other Government agencies, or partners of those organisations, on a statutory basis. This data sharing underpins college funding and educational attainment policy and monitoring.

Student email accounts

During the application process, we will contact you using the telephone and personal email address that you provided during the application process. As soon as you have enrolled and received your student ID card, you will have a college IT created with a student email account. All subsequent email correspondence will be via your College email account (regardless of age). Student personal email addresses will not be used.

Data collection requirements:

To understand what learner personal data is collected by the DfE, through the ESFA, and how it is handled, go to:

guidance.submit-learner-data.service.gov.uk/24-25/ilr/ilrprivacynotice

To find out more about the statutory data collection requirements placed on us by DfE and its agencies, go to:

https://www.gov.uk/education/data-collection-for-further-education-providers

Youth support services

Students aged 16+:

We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit your local authority website.

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils and students in schools and colleges in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools and colleges, local authorities and awarding bodies.

We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the Individualised Learner Record (ILR). Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to pupil and student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

For information about which organisations the department has provided student information, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, students have the right to request access to student information that we hold. To make a request for your personal information, contact rmurray@buckscollegegroup.ac.uk

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/ or telephone: 0303 123 1113.

Contact

If you would like to discuss anything in this privacy notice please contact foi@buckscollegegroup.ac.uk

PRIVACY NOTICES: ONLINE LEARNING AND LIVE LESSONS

Data Use
We want to ensure that students are able to access a variety of online learning including 'live lessons' which will include a mixture of teaching and instruction and also giving students tasks to complete.

These lessons will be hosted via online video platforms such as Microsoft Teams. When accessing these platforms, students will need to share some basic personal information in order to use the platform (i.e. name and agreed email address). It is very important that your personal information is kept safe and there are measures in place to ensure this happens.

You can find details on the information required by individual video platforms and their security measures by viewing their privacy notices. Examples of the video platforms used are as below:
Microsoft Teams: https://www.microsoft.com/en-gb/microsoft-365/microsoftteams/security

When students take part in online live lessons, aspects of your personal data (i.e. name and email address) will be shared with third parties such as the above video platforms, which is required in order for these systems to be accessed. These systems relate to our public task to provide pupils with an education.

Safety and Security
We have a number of measures in place to mitigate against the potential misuse of students personal data and to ensure the live lessons are accessed safely. These include:

- All staff hosting 'live lessons' will use their Buckinghamshire College email accounts.
- All students will be required to access our Virtual Learning Environment (Cloud) and/or use their College email account to access live lessons.
- All lessons will be password protected with the access link placed in a secure location.
- Sessions may be recorded by staff. In these instances, students will consent to this recording being made by clicking a button on their screen.
- The 'waiting room' feature will be used by the staff member to allow for a controlled admittance of pupils by the host when ready.
- Users will be identified prior to admittance to the live lesson.
- Staff and students will not share files that could contain viruses or malware.
- Staff will not allow other users to control the screen. Students may be asked to share their screen if requested by the tutor.
- The live lesson link will be confidential and will be available to members of that course only
- Students will not be allowed to record or take screen shots of the live lessons.
- Students may be invited to 1:1 sessions for the following reasons:
  - Learning support
  - Safeguarding meetings
  - To provide feedback either from your vocational tutor or via tutorial sessions

  1:1 sessions should be agreed in advance and may be recorded, with consent, as a record of the session if deemed necessary. If the student does not wish to participate in 1:1 sessions the tutor should make alternative arrangements.
- Staff and students must wear suitable clothing, as should anyone else in the household.
- Any computers used should be in appropriate areas, and where possible be against a neutral background.
- All language must be professional and appropriate, including any family members in the background.
- Videos may be muted from both pupils and staff if other members of the household become unsettled or cause disruption.

The General Data Protection Regulations (GDPR) The General Data Protection Regulations (GDPR) provide a framework of Articles about the use of personal data. We have included a cross reference to the relevant Articles in the information below. The use of your information for these purposes is lawful for the following reasons:

- We are under a legal obligation to collect the information or the information is necessary for us to meet legal requirements, such as our duty to safeguard pupils. (Article 6, 1c)
- It is necessary for us to hold and use the information for the purposes of providing education and so we can look after our students. This function is in the public interest because everybody needs to have an education. (Article 6, 1e)
- Sometimes we need permission to use certain information. In these circumstances, we will ask you, for permission. (Article 6, 1a)

Concerns
If you have any specific queries or concerns about the data processing required in order for your access live online lessons, then please speak to your teacher in the first instance, and ask them to contact College Data Protection Officer. If necessary, you can contact an outside agency - the Information Commissioner's Office who could also help at https://ico.org.uk/concerns/

Appendix 2 – Personal Data Breach Notification Policy

1. OVERVIEW

The Buckinghamshire College Group's reputation and future growth are dependent on the way the College manages and protects Personal Data. As an organisation that collects and uses Personal Data, the College takes seriously its obligations to keep that Personal Data secure and to deal with security breaches relating to Personal Data when they arise. The College's key concern in relation to any breach affecting Personal Data is to contain the breach and take appropriate action to minimise, as far as possible, any adverse impact on any individual affected. The College has therefore implemented this Policy to ensure all College Personnel are aware of what a Personal Data reach is and how they should deal with it if it arises.

This Policy is available to all staff on the College Intranet and will form part of the induction for new staff. All staff will receive notification of periodic revisions of this Policy. This Policy does not form part of any College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All College Personnel are obliged to comply with this Policy at all times.

2. ABOUT THIS POLICY

This Policy explains how the College complies with its obligations to recognise and deal with Personal Data breaches and (where necessary) to notify the ICO and the affected individuals. The College has a corresponding Data Breach Notification Procedure and Data Breach Register that set out how the College deals with and records Personal Data breaches.

3. SCOPE

This Policy applies to all College Personnel who collect and/or use Personal Data relating to individuals.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

4. DEFINITIONS

4.1. **College** – Buckinghamshire College Group

4.2. **College Personnel** – Any College employee or contractor who has been authorised to access any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

4.3. **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.

4.4. **Data Protection Officer** – The Data Protection Officer is the Director of MIS and Planning and can be contacted at RMurray@buckscollegegroup.ac.uk

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

4.6. **Personal Data** – any information about an individual, which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

4.7. **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.

5. WHAT IS A PERSONAL DATA BREACH

5.1. 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.

5.2. 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. 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 internal does.

5.3. A Personal Data breach could include any of the following:

5.3.1. loss or theft of Personal Data or equipment that stores Personal Data;

5.3.2. loss or theft of Personal Data or equipment that stores the College's Personal Data from a College supplier;

5.3.3. inappropriate access controls meaning unauthorised College Personnel can access Personal Data;

5.3.4. any other unauthorised use of or access to Personal Data;

5.3.5. deleting Personal Data in error;

5.3.6. human error (which could be as simple as putting a letter in the wrong envelope or leaving a phone or laptop containing Personal Data on a train);

5.3.7. hacking attack;

5.3.8. infection by ransom ware or any other intrusion on our systems/network;

5.3.9. 'blagging' offences where information is obtained by deceiving the organisation who holds it; or

5.3.10. destruction or damage to the integrity or accuracy of Personal Data.

5.4. A Personal Data breach can also include:

5.4.1. equipment or system failure that causes Personal Data to be temporarily unavailable;

5.4.2. unforeseen circumstances such as a fire, flood or power failure that causes Personal Data to be temporarily unavailable;

5.4.3. inability to restore access to Personal Data, either on a temporary or permanent basis; or

5.4.4. loss of a decryption key where Personal Data has been encrypted because this means the College cannot restore access to the Personal Data.

6. REPORTING A PERSONAL DATA BREACH

6.1. College Personnel must immediately notify any Personal Data breach to the Data Protection Officer, no matter how big or small and whether or not College Personnel think a breach has occurred or is likely to occur. This allows the College to contain the breach as soon as possible and to consider a recovery plan to minimise any risk of damage to the individuals affected and to the College.

6.2. If College Personnel discover a Personal Data breach outside working hours, College Personnel must notify it to the College's Data Protection Officer as soon as possible.

6.3. College Personnel may be notified by a third party (e.g. a supplier that processes Personal Data on the College's behalf) that they have had a breach that affects College Personal Data. College Personnel must notify this breach to the College's Data Protection Officer and the College's Data Breach Notification Procedure shall apply to the breach.

7. MANAGING A PERSONAL DATA BREACH

7.1. There are four elements to managing a Personal Data breach or a potential one and this Policy considers each of these elements:

7.1.1. Containment and recovery

7.1.2. Assessment of on-going risk

7.1.3. Notification

7.1.4. Evaluation and response

7.2. At all stages of this Policy, the Data Protection Officer and managers will consider whether to seek external legal advice.

8. CONTAINMENT AND RECOVERY

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

8.2. 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.

8.3. 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 bespoke Personal Data breach plan to address the breach concerned in accordance with the College's Data Breach Notification Procedure. This will include consideration of:

8.3.1. 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;

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

8.3.3. 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.

8.4. 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.

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

9. 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 consider the on-going risks to the College and to any other party caused 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.

10. NOTIFICATION

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

10.2. 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.

10.3. 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.

10.4. 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.*

10.5. Please note that 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.

10.6. 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.

10.7. 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.

10.8. 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.

10.9. 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.

10.10. The College may not be required to notify the affected individuals in certain circumstances as exemptions 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.

11. EVALUATION AND RESPONSE

11.1. 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.

11.2. 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 Personal Data Breach Register.

11.3. 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.

Equality Impact Assessment

Section One	
College:	Buckinghamshire College Group
Departments Effected:	Whole college
Who is responsible for the Equality Impact Assessment?	Executive Director Digital Transformation and Planning
Title (of the policy/practice/decision)	General Data Protection Policy
Description (Provide a brief description of the policy/practice/decision)	The **General Data Protection Policy 2024-27** ensures Buckinghamshire College Group manages and protects personal data in compliance with GDPR and the Data Protection Act 2018, covering data security, individual rights, and lawful data processing.

Section Two – Stakeholder Consultation		
2	Who are the main stakeholders and what consultation exercise are you planning to undertake, if required (e.g. consultation with Employee Voice, Trades Unions, Staff groups, Student groups?	The main stakeholders for the **General Data Protection Policy 2024-27** are College Personnel, students, suppliers, governors, parents, visitors, and the Data Protection Officer, along with local authorities and government agencies.
3	Are there concerns that this could result in differential or adverse impact on any Equality Groups (Protected Characteristics as identified by the Equality Act 2010)	There are no concerns. The policy includes measures to ensure fair and equitable treatment of all individuals, with reasonable adjustments made as part of the risk assessment process to accommodate the needs of different groups.

Section Three
Please identify how the policy may impact the following protected characteristics:

- Identify any positive impacts the policy/practice/decision may have on equality groups.
- Identify any negative impacts the policy/practice/decision may have on equality groups.
- Propose measures to mitigate or eliminate identified negative impacts.

Protected Characteristics	**Impact** **High/Medium/ Low/N/A**	**Action(s) you will take to mitigate or remove the negative or adverse impact if identified?** Propose measures to mitigate or eliminate identified negative impacts
1. Age *(e.g. are there ways older or younger people may find it difficult to engage?)*	High - positive	
2. Disability *(eg do you need to consider large print or easy read?)*	High - positive	
3. Gender identification *(eg is your language inclusive of LGBTQ+ groups?)*	Medium - positive	
4. Gender Re-assignment *(eg is your language inclusive of trans and non-binary people?)*	Medium - positive	
5. Marriage and civil partnership *(eg does it treat marriage and civil partnerships equally?)*	n/a	
6. Pregnancy & Maternity *(eg with this have an impact on pregnant or those on family leave; breastfeeding services?)*	Medium - positive	
7. Race / Ethnicity	Medium - positive	

(eg does it take into account the needs of people from different groups)		
8. Religion or Belief *(eg do people from faith groups experience any specific disadvantage)*	Medium - positive	
9. Sexual Orientation *(eg is your language inclusive of LGBTQ+ groups?)*	Medium - positive	

Section Four – Monitoring and Review	
Does your criteria and procedure promote fairness and equal opportunities? *Utilize relevant data sources, such as demographic information, student feedback, or staff surveys, to inform the analysis as necessary*	Yes, the General Data Protection Policy 2024-27 promotes fairness and equal opportunities by ensuring that personal data is processed lawfully, fairly, and transparently. The policy includes measures to protect the rights of all individuals, regardless of their protected characteristics, and mandates reasonable adjustments to accommodate the needs of different groups. This approach helps to ensure equitable treatment and access to data protection rights for everyone.
How will you monitor and evaluate the effectiveness of these measures to determine whether it has been effectively and fairly applied	Requests and data breach records will be analysed against equality, diversity and inclusion measures and any trends reported to the Executive team

Section Five – Outcome, Sign-off and Authorisation	
Equality Impact Assessment Outcome Select one of the four options below to indicate how the development/review of the policy/practice will be progressed and state the rationale for the decision	
Option 1: No change required – the assessment is that the policy/practice is/will be robust.	Y
Option 2: Adjust the policy or practice – this involves taking steps to remove any barriers, to better advance equality and/or to foster good relations.	
Option 3: Continue the policy or practice despite the potential for adverse impact, and which can be mitigated/or justified	
Option 4: Stop the policy or practice as there are adverse effects cannot be prevented/mitigated/or justified.	
Name & job title of authorised person	Rachael Murray, Executive Director Digital Transformation and Planning
Equality Impact Assessment was completed on:	October 2024
Date of next review, and by whom? This may include regular reviews, data analysis, and stakeholder feedback	June 2027 by Executive Director Digital Transformation and Planning