William College

Data Protection Policy

Table of Contents

1. Introduction

William College is committed to complying with the General Data Protection Regulation in its role as an academic institution, employer, and service provider.
To uphold this commitment, the College ensures that data is processed fairly and legally, supports the rights of individuals, maintains the security of personal data, and integrates privacy considerations into its systems and processes.
This policy outlines how William College handles the personal data of students, staff, Governors and Directors, suppliers, website users, and other third parties, in full compliance with relevant data protection legislation.

2. Legal Framework

The Data Protection Act 2018 ('DPA 2018') sets out the framework for data protection law in the UK.

The UK General Data Protection Regulation ('UK GDPR') is a UK law which came into effect on 1 January 2021. It sets out the key principles, rights and obligations for most processing of personal data in the UK.

The Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights. It offers advice and guidance, promotes good practice, considers complaints, and takes enforcement action where appropriate. The ICO can be contacted at https://ico.org.uk/make-acomplaint/. William College's registration number is **ZB681561**.

Included within Appendix A is a set of definitions for key terminology in relation to data protection. Included within Appendix B and Appendix C are the lawful bases for processing any personal data and special categories of personal data.

3. Purpose and Scope

The College holds and processes personal data for various purposes, including admissions, academic services, statutory returns, and employment administration. It also includes a subset of personal data known as special category data, which includes sensitive information such as racial or ethnic origin, health data, and sexual orientation.

This Policy outlines how the institution handles personal data of staff, students, and third parties and it applies to all staff members, contractors, and students who handle personal data. Compliance with this policy is mandatory and any breach may result in disciplinary action.

4. Data Protection Principles

William College is committed to processing personal data in accordance with the core principles outlined in Article 5(1) of the UK General Data Protection Regulation (UK GDPR). These principles form the foundation of the Data Protection Act 2018 and establish the legal framework for handling personal data.

In line with the Data Protection principles[1], William College will ensure that personal data is:

I. **Lawfulness, Fairness and Transparency** - Processed lawfully, fairly and in a transparent manner in relation to the data subject.

The College's Privacy Notice sets out clearly and publicly how the Institute collects, uses and shares prospective, current and former student's data, and for what purpose. The same notice seeks to help students understand their rights in relation to the personal data the College holds. This ensures that students can make an informed decision about whether or not to provide the data requested.
Staff consent to the processing by William College of their personal data as necessary for the performance of their Contract of Employment and/or the conduct of William College's business, including

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

their partners, technology suppliers, government and other public bodies if required. Detailed coverage of data protection matters is provided in individual staff contracts.

All staff at William College who process personal data about students, staff, applicants, alumni or any other individual must comply with the requirements of this policy.

II. **Purpose Limitation** - Collected only for specified, explicit and legitimate purposes.

William College only processes personal data for the specific purposes explained to the data subject at the point of collection. Should the College need to use the data for a different and unrelated purpose, the data subject will be informed before any processing takes place. In some cases, consent of the data subject may be required.

III. **Data Minimisation** - Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

William College seeks to collect or process only the minimum amount of personal data required to properly achieve the purpose in question and consider the use of anonymised or pseudonymised data. Information which is not needed or is not relevant for a purpose will not be collected or otherwise processed. Collecting personal data "just in case" for future reference is not compliant with the legislation.

IV. **Accuracy** - Accurate and, where necessary, kept up to date.

The accuracy of personal data is verified at the point of collection and regularly thereafter. Inaccuracies are corrected or erased, as appropriate; however, information will not be deleted if it has been used to inform decisions affecting a data subject. In such cases, the information will be corrected for future use (to ensure it is up to date) and an explanatory note will be added.
Quality of data is verified before transmission – William College will not transmit any data that is inaccurate, incomplete or no longer up to date

V. **Storage Limitation** - Not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed.

Personal data is not kept for longer than necessary and is securely handled to protect against unauthorised access or loss.
William College will destroy (securely) or erase data from our systems when there is no longer a legal, business or operational requirement for it to be retained, taking into account the purposes for which it was originally requested it.

VI. **Integrity and Confidentiality** - Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

William College protects its personal data against unauthorised access, loss or destruction by a range of security measures. All College's systems and services are fully cloud-based, and we exclusively use a third-party cloud storage provider, with whom we have contractual agreements, which includes secure hosting within the UK or regions compliant with UK data protection regulations.
All systems are subject to regular vulnerability scans, and security patches must be up to date for IT systems which are being designed and delivered by third-party suppliers prior to becoming operational, as set out in our System Management Policy.

Our Information Security Policy supports compliance by ensuring appropriate technical measures are in place to protect personal data. All staff should ensure that any personal data, which they hold, is kept securely and that personal information is not disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. All personal information in the form of manual records should be kept in a locked filing cabinet or kept in a locked drawer, in a lockable room where access is limited to relevant staff only.

Personal data must not be transferred outside of the UK, including the use of websites or applications hosted on servers based outside of the UK, unless appropriate safeguards are in place.

VII. **Accountability** - The controller shall be responsible for, and be able to demonstrate compliance with, the first principle.

The College will maintain appropriate records to demonstrate compliance with these principles.

4.2 Data protection by design and default

William College is committed to data protection by design and default, ensuring that personal data is processed with the highest privacy protection.

Data protection by default is linked to the fundamental protection principles of data minimisation and purpose limitation whereby we are required to ensure that personal data is processed with the highest privacy protection and not made accessible to an indefinite number of persons.

Data protection by design is the practice of anticipating and embedding data protection measures within any project (e.g. collecting a new type of data or implementing a new system or process for holding or accessing personal data) from the outset. This ensures that security is a key consideration rather than an after-thought. Data protection by design is closely linked with the requirement for record-keeping and accountability.

All staff must use the minimum amount of data necessary for the purpose and consider the use of anonymised data or pseudonymised data, as appropriate.

5. Data Subject Rights

Data Subjects – our students, staff and third parties - have the right to exercise their rights under GDPR[2].

I. **The right to be informed** (Privacy Notice)

Data Subjects have the right to be informed about the collection and use of their personal data.

Data Subjects have the right to clear and concise information about what will be done with their personal data. The Privacy Notice publicly available on William College's website explains how the College collects, uses and shares personal data, and an individual's rights in relation to the personal data held. Staff consent to the processing by William College of their personal data as required for fulfilling their Contract of Employment and supporting the College's operations. Detailed coverage of data protection matters is provided in individual staff contracts.

II. **The right to subject access** (subject access request)

Data subjects have the right to access and receive a copy of their personal data, and any other information held about them and to be assured that the processing of their data is fair and lawful. Such requests must be referred to our Data Protection Officer who will ensure a response is provided to valid requests within one month of receipt. No such rights exist, however, in relation to exam scripts and exam marks.

Although individuals are able to obtain a copy of their personal data free of charge, the College reserves the right to charge for any additional copies. We are only able to charge a fee if we think the request is manifestly unfounded or excessive. If so, it would be reasonable for us to charge a fee for administrative costs associated with the request.

For information about the right of access and Subject Access Request, see our Subject Access Request Policy.

III. **The right to rectification**

[2] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/

The UK GDPR includes a right for Data Subjects to have inaccurate personal data rectified or completed if it is incomplete.

William College makes every effort to ensure its data is accurate. If a Data Subject thinks something we hold about them is wrong, they can ask for this to be corrected. The College will assess the request and correct any inaccuracy. In some circumstances, if personal data is incomplete, the data subject can also require the controller to complete the data, or to record a supplementary statement.

Such requests must be referred to our Data Protection Officer who will ensure a response is provided to valid requests within one month of receipt.

IV. The right to erasure (the right to be forgotten)

The UK GDPR introduces a right for Data Subjects to have personal data erased. The right is not absolute and only applies in certain circumstances. This only applies:

- where the data is no longer required for the purpose for which it was originally collected or processed, or
- where the data subject withdraws consent, or
- where the data is being processed unlawfully.

The right to erasure does not apply if processing is necessary to:

- exercise the right of freedom of expression and information
- comply with a legal obligation
- perform a task carried out in the public interest or in the exercise of official authority
- archive in the public interest, scientific research, historical research or statistical purposes, where erasure is likely to make achievement of that processing impossible or disproportionately difficult
- establish, exercise or defend legal claims

Such requests must be referred to our Data Protection Officer who will ensure a response is provided to valid requests within one month of receipt.

V. The right to restrict processing

Data Subjects have the right to request the restriction or suppression of their personal data. This means that data subjects may not wish to have their data erased but rather have any further processing restricted. However, this is not an absolute right and only applies in certain circumstances.

- the individual contests the accuracy of their personal data and the College is verifying it
- the data has been unlawfully processed
- the personal data is no longer needed but the individual needs it retained in order to establish, exercise or defend a legal claim
- the individual has objected to the processing their data, and the Institute is considering whether any legitimate grounds override this

VI. The right to portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. This allows Data Subjects to move, copy or transfer personal data easily from one IT environment to another, i.e. another data controller, in a safe and secure way, without affecting its usability. This only covers data submitted by the subject, or data captured on the subject's use of a service, for example, use of online services like our VLE. If technically possible, the College will consider transferring information directly to another organisation.

VII. The right to object

The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. Individuals have the right to object to specific types of processing, such as processing for direct marketing, research or statistical purposes. The data subject must demonstrate grounds for objecting to the processing, except in the case of direct marketing where it is an absolute right.

VIII. The right to automated decision-making and profiling

The UK GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

In the case of automated decision-making and profiling that may have significant effects on data subjects, data subjects have the right to either have the decision reviewed by a human being or to not be subject to this type of decision-making at all. These requests must be forwarded to the Data Protection Officer immediately.

These rights are not absolute and can be further explored through the Information Commissioner's Office (ICO).
Where an individual makes a request relating to any of the rights listed above, we will consider each such request in accordance with all applicable Data Protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject. Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative.

6. Roles and responsibilities

The **Data Protection Officer** (DPO) has overall responsibility for data protection compliance. The DPO has those responsibilities laid out in Article 39 of the UK General Data Protection Regulation (UK GDPR). The DPO can be reached at dpo@williamcollege.com.

All **Heads of Departments and Line Managers** are responsible for ensuring that Personal Data in their area is processed in accordance with this Policy and any associated regulations, policies, and procedures and that staff within their area have completed mandatory data protection training. Heads of Divisions/Departments are responsible for ensuring that staff within their area of responsibility apply appropriate practices, processes, controls to comply with this policy.

All staff at William College who process personal data about students, staff, applicants, alumni or any other individual must comply with the requirements of this policy. This includes:

- personal information is not disclosed by them either orally or in writing, to any unauthorised third party
- they do not access any personal data which is not necessary for carrying out their work
- personal data in paper format is kept in a secure place when not being processed
- personal data on computer should not be accessed or viewed by unauthorised staff or students and as such workstations must be locked or password protected when not in use
- where personal data is held on paper, this should not be removed from the College
- staff processing personal data for research purposes should include a Data Protection Privacy Notice informing the data subject, in this case a research participant, of as the following:
    - What data is being collected
    - Why the data is being collected
    - The legal basis for processing
    - How long it will be retained for
    - Rights of the participants
    - Who to contact when they need to exercise their rights or complain as a participant. To complain about the research itself, the appropriate contact will be the team/person conducting the research. To enforce their rights, the contact is the Data Protection Officer dpo@williamcollege.com.

Students may need to process personal information for project or research purposes which include the collection and processing of personal data. This can include activities such as questionnaires, surveys,

and focus groups where participants are interviewed. In carrying out these activities, students have the same responsibilities as staff as stated above.
Students must ensure that they are familiar with the Privacy Notice published on our website and ensure that any information they provide to William College is kept up to date.

Where external companies are used to process personal data on our behalf, responsibility for the security and appropriate use of that data remains with William College.

7. Data Protection Impact Assessments (DPIAs)

William College recognises its obligations under the UK General Data Protection Regulation (UK GDPR) to assess data protection risks associated with high-risk processing activities. A Data Protection Impact Assessment (DPIA) is a tool used to systematically identify, assess, and mitigate the potential risks to the rights and freedoms of individuals arising from certain types of personal data processing.

7.1 When a DPIA is Required

A DPIA will be undertaken where processing is likely to result in a high risk to individuals. This includes, but is not limited to, the following types of processing:

- Systematic and extensive profiling or automated decision-making
- Large-scale processing of special category data or criminal offence data
- Systematic monitoring of publicly accessible areas
- Use of new or innovative technologies
- Processing involving vulnerable individuals (e.g. children)
- Data matching or combining datasets from different sources
- Processing that may prevent individuals from exercising a right or using a service

Where there is uncertainty about whether a DPIA is required, advice will be sought from the Data Protection Officer (DPO). A precautionary approach will be adopted, and a DPIA will be conducted where appropriate.

7.2 DPIA Procedure

Staff proposing a new processing activity will engage the DPO at the earliest possible stage to determine whether a DPIA is necessary. If so, the following steps will be undertaken:

1. Describe the nature, scope, context and purpose of the processing
2. Assess the necessity and proportionality of the processing
3. Identify and assess potential risks to individuals' rights and freedoms
4. Describe measures to mitigate those risks and reduce them to an acceptable level
5. Record the outcome and ensure integration into the project plan

The DPO will provide advice and guidance throughout the process. All DPIAs must be approved by the SLT or senior manager.

7.3 Documentation and Review

A record of completed DPIAs will be maintained and retained by the DPO in accordance with the William College's Records Management Policy. DPIAs will be reviewed periodically and whenever there is a substantial change to the nature, scope, or purpose of the processing activity.

7.4 Consultation with the ICO

Where a DPIA identifies a high risk that cannot be mitigated, William College will consult the Information Commissioner's Office (ICO) before proceeding with the processing activity.

8. Data sharing

When introducing a new data sharing process, it is essential to ensure compliance with data protection legislation. This may include carrying out a Data Protection Impact Assessment (DPIA) to evaluate potential privacy risks and, where appropriate, putting in place a formal data sharing agreement. The Information Commissioner's Office (ICO) provides a Data Sharing Code of Practice to support organisations in sharing personal data lawfully, fairly, and transparently.

Personal data may also be shared within the organisation, provided there is a legitimate business purpose and the sharing aligns with the principles of the UK GDPR.

8.2 Transfers of personal data outside the UK

The UK GDPR restricts transfers of personal data outside the UK unless individual rights are protected, or specific exceptions apply. Transfers to countries covered by UK "adequacy regulations" are permitted, including all countries within the EEA, Andorra, Argentina, Gibraltar, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, and Uruguay.
William College does not host or transfer any personal data outside of the UK or to countries not covered by the UK adequacy regulations.

9. Recordkeeping

Key information such as name, course details, and contact information is recorded for administrative purposes. This data may be stored on paper or electronically and is used for scheduling appointments, generating anonymised statistical reports, and supporting a high-quality student experience both academically and personally. Correspondence and documents submitted by applicants or students may be attached to these records.

The relevant senior manager is responsible for maintaining centralised records to meet the needs and reasonable expectations of students, the College, and external bodies. For staff members, this responsibility lies with Human Resources.

To minimise duplication and enhance data security, central databases such as the Student Records System should be used. Any locally maintained databases containing personal data—including those using reference numbers in place of names—must be kept secure.

The College must ensure all data is accurate and up to date. Staff and students are responsible for regularly updating their personal records through the appropriate system.

Sensitive information provided by applicants or students may be retained to ensure appropriate advice or responses. Staff may share relevant information with colleagues or third parties where necessary to address concerns or support wellbeing.

Academic records—including module and programme results, coursework, placements, and practice outcomes—may be shared with relevant academic and administrative staff and awarding bodies for the purposes of approving marks, determining progression, and issuing awards.

Under the UK General Data Protection Regulation (UK GDPR), the College is required to maintain full and accurate records of its data processing activities, including consent records where applicable. These records must include:

- The name and contact details of the College as a Data Controller and the Data Protection Officer
- Clear descriptions of:
    - the personal data types we collect
    - the processing activities with which we engage
    - processing purposes
- Any third-party recipients of personal data
- Personal data storage locations
- Personal data transfers

- The retention schedule for personal data
- A description of the security measures in place for personal data including special categories of personal data.

Additionally, the College is required to maintain records of any personal data breaches, including the circumstances involved and actions taken in response.

10. Confidentiality

Information received and recorded by William College is treated with sensitivity, in absolute confidence and with care and discretion. It is only used for the purposes for which it was provided, and staff will not disclose any personal information to third parties without the student's express written permission, subject to the following exceptions:

- Legal obligations, such as court of law, police, other law enforcement agencies or a written request under the Data Protection Act.
- Concerns for welfare or risk of harm to self or others.
- Sharing anonymous statistical data, for example data that cannot be used to identify any individuals

11. Data retention and disposal

The Data Protection Act 2018 requires William College to retain personal data for operational purposes, while ensuring compliance with data protection principles. This is done while remaining compliant with the Data Protection Principle which requires that personal data are not kept longer than is necessary for their purpose.

Personal data must not be kept longer than necessary for the purposes for which it was originally collected. This applies to all personal data, whether held on core systems, local PCs, laptops or mobile devices or held on paper. If the data is no longer required, it must be securely destroyed or deleted.

William College will securely destroy or erase notes and information from systems when there is no longer a legal, business or operational requirement to be retained, taking into account the purposes for which the information was requested. All staff have a responsibility to consider safety and security aspects when disposing of personal data in the course of their work. Consideration should also be given to the nature of the personal data involved (how sensitive it is), and the format in which it is held.

12. Liaison and Correspondence

In certain cases, staff may need to contact a third party on behalf of an applicant or student to address their concerns or enquiries. However, staff will only initiate contact with written permission from the applicant or student, except in exceptional circumstances. If permission is granted, the nature of the contact will be agreed upon in advance. Staff will not disclose personal information without permission, except in emergencies or exceptional circumstances:

- Where there is a legal obligation, for example to release information to the Police, a court of law, Student Funding Companies, the UK Visas and Immigration (UKVI) or other law enforcement agencies. A written request made under the Data Protection Act 2018 will normally be required before this information is released.
- If the applicant or student is under 18 years of age and William College has serious concerns about their welfare.
- If William College has significant concerns that the applicant or student presents a risk of harm to self or to others.
- For statistical data, for example data that cannot be used to identify any individuals, this could be shared anonymously across the Institute to help spot trends and plan services

If staff are unsure to whom they can legitimately disclose personal data, they should seek advice from the Data Protection Officer at dpo@williamcollege.com.

13. Students with a disability, longer-term medical condition, or specific learning difficulty

If a student has declared a disability, long-term medical condition or specific learning difficulty, under the UK's Equality Act 2010, William College is legally required to make reasonable adjustments to support students to participate to the fullest extent possible in the educational opportunities provided by the College.
Students' information will only be shared with their consent. If the student does not give permission, this may seriously limit the scope and nature of any adjustments that William College can make on behalf of the student.

14. Data Breach Management

William College emphasises the importance of staff training and personal responsibility for compliance with data protection legislation.

William College makes every effort to avoid data protection incidents, however, it is possible that mistakes will occur on occasions. Examples of personal data incidents might occur through:

- Loss or theft of data or equipment
- Ineffective access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

All breaches of data protection should be reported to the Data Protection Officer using the incident report form (see Appendix D) should be completed and should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. An assessment will be made as to whether there are significant risks to the rights and freedoms of individuals and whether a notification must be made to the Information Commissioner's Office. Any such notification must be approved by the Data Protection Officer and reported within 72 hours of the notification of the breach.
It is essential that staff report a breach or potential breach immediately. This allows quick action to be taken to address the breach, as well as allowing the College to comply with its obligation to report breaches.

If there has been clear negligence or intent with regard to any breach of the data protection policy by members of staff or students, the College will consider the circumstances and decide how best handle the next steps. Where a staff member has been negligent without mitigation, this will be dealt with in accordance with the College's Staff Disciplinary Policy. All factors will be taken into account when determining appropriate action, including whether the beach was reported promptly.

Once a data breach has been reported an initial assessment will be made to establish the severity of the breach. Breaches can result in disciplinary action, criminal prosecution, and fines of up to 4% of annual global turnover or up to £20 million.

15. Making a complaint

The College is committed to handling personal data in accordance with the legislative framework.
Concerns or complaints about the College's handling of personal data should be directed to the Data Protection Officer at: dpo@williamcollege.com.
All Data Subjects have the right to make a complaint about our handling of personal data to the Information Commissioner's Office: https://ico.org.uk/make-a-complaint/.

16. Equality Statement

This policy reflects the provisions set out in the Equality Act 2010 which ensures no less favourable treatment based on protected characteristics and respects human rights.

17. Review of the Policy

This policy is reviewed annually by the Senior Leadership Team and may be triggered by legislative changes. Any amendments require the approval of our Board of Governors.

18. Related Internal Policies and External Reference Points

Internal Policies

- Information Security Policy
- System Management Policy
- Student Records Retention Policy
- Privacy Notice
- Data Subject Access Request Policy
- Staff Disciplinary Policy
- Student Complaints Policy
- Student Disciplinary Policy

External Reference Point:

- Equality Act 2010
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Equality Act 2010

March 2025

Appendix A: Definitions

This section provides definitions and explanations of important terms related to data protection.

Personal Data	Any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an address, a student number, an IP address, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data may also include special categories of personal data (see below). These are considered to be more sensitive and may only be processed in more limited circumstances.
Special Category Data	Sensitive data that requires extra protection. Special category personal data relates to an individual's race, ethnicity, political opinion, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation.
Anonymisation and Pseudonymisation	If personal data can be truly anonymised, then the anonymised data is not subject to data protection legislation. If this is not possible, it is advisable to aim for partial anonymisation or pseudonymisation of data. Pseudonymisation involves the separation of personal data from direct identifiers so that no connection to an individual can be made without additional information that is held separately. Although partially anonymised and pseudonymised data are not exempt from data protection legislation, we recognise that they provide an added layer of security for the handling and processing of data.
The Data Controller	The individual/organisation registered with the Information Commissioner who is responsible for ensuring compliance with the requirements of the Data Protection Act 2018 and UK GDPR. This includes determining the purpose(s) for which personal data are collected and processed, and the means by which that data is processed. William College is the Data Controller.
Data Processors	Any individual or organisation who processes personal data on behalf of – and according to the purposes defined by – the Data Controller.
Data Protection Officer	The person appointed as such under the UK GDPR and is responsible for advising the Institution (including its employees) on their obligations under Data Protection Law, for monitoring compliance with data protection law, as well as with the Institution's polices, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.
Processing	Anything that is done with personal data, including collection, storage, use, disclosure, and deletion.
Data Protection Impact Assessment (DPIA)	Is a tool used to identify and reduce risks in processing activities.
Consent	Is the freely given, specific, informed, and unambiguous indication of a data subject's wishes for the processing of their personal data.
EEA	Refers to the 28 countries in the European Union and Iceland, Lichtenstein, and Norway.
Data Subjects	An identifiable living person who can be identified, directly or indirectly from personal data. This may include current, prospective and former staff or students, suppliers of goods and services, business associates, etc.

Appendix B: The lawful bases for processing any personal data

The College must meet one or more of the following six legal bases in order to be able to process personal data:

- the data subject has given **consent** to the processing for one or more specific purposes. This consent must be provided by way of a positive action, and a record of consent must be maintained. It must be as easy for the subject to opt out as it was for them to opt in.
- processing is necessary for the performance of a **contract** or to take steps, at the request of the data subject, prior to entering into a contract; for example, processing carried out by the College in order to provide services to subjects, including staff and students.
- processing is necessary for compliance with a **legal obligation**. There must be a specific piece of legislation which requires the personal data to be processed.
- processing is necessary in order to protect the **vital interests** of an individual. This is mainly relevant in 'life or death' situations only.
- 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 College. The College may be able to rely upon this for any activities carried out under its public function, such as the retention of student transcripts and the management of staff.
- processing is necessary for the purposes of the **legitimate interests** pursued by the College, except where these interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Due to its sensitive nature, the College must fulfil further conditions, in addition to the above, in any circumstances in which Special Category Data is being processed. These conditions are set out in the Data Protection Laws.

Appendix C: The lawful bases for processing special categories of personal data

The lawful bases for processing special categories of data are outlined in Article 9 of the UK GDPR and supplemented by conditions in the Data Protection Act 2018. When processing special categories of data, at least one condition from Article 6 and one from Article 10 of the UK GDPR must be met. These conditions include:

- The data subject has given explicit consent.
- The processing is necessary for the purposes of employment, social security and social protection law.
- The processing is necessary to protect someone's vital interests (either the data subject or another natural person) where the data subject is physically or legally incapable of giving consent.
- The processing is manifestly made public by the data subject.
- The processing is necessary for legal claims or whenever courts are acting in their judicial capacity.
- The processing is necessary for reasons of substantial public interest.
- The processing is necessary for the purposes of medicine, the assessment of the working capacity of the employee, the provision of health or social care or treatment or the management of health or social care systems and services.
- The processing is necessary for public health.
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to certain safeguards.

Appendix D: Incident reporting form

One must act promptly to report any data breaches (or potential data breaches/near miss). If a data breach or near-miss is discovered, the relevant head of division/department must be notified, and a completed form (below) returned to dpo@williamcollege.com.

Description of breach:	
Time data breach was identified and by whom:	
Time data breach occurred and by whom:	
Who is reporting the breach?	
Name/post/department:	
Email address:	
Classification of data breached (in accordance with the breach policy): **Public data** **Internal data** **Restricted Data** **Confidential Data**	
Volume of data involved (number of people effected):	
Is the breach contained or ongoing?	
What actions are being/have been taken to recover the data?	
Any other relevant information:	