ASKHAM BRYAN COLLEGE

Data Protection Policy 2025 – 2026 (Updated)

Equality Impact Assessment: Askham Bryan College recognises the importance of the Equality Act 2010 and its duties under the Act. This document has been assessed to ensure that it does not adversely affect staff, students or stakeholders on the grounds of any protected characteristics.

1. PURPOSE

1.1 Data Protection in the UK is primarily governed by 2 key pieces of legislation: the Data Protection Act 2018 (or "DPA 2018") and the UK GDPR. There is other legislation dealing with data protection, such as the Law Enforcement Directive (Directive (EU) and the Privacy and Electronic Communications Regulations 2003 (PECR); but the DPA 2018 and UK GDPR are the Acts most frequently referred to when talking about "data protection".

1.2 The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998, and came into effect on 25th May 2018, at the same time as the EU GDPR, which has since been replaced in the UK by the UK GDPR (see 1.3). The Act seeks to empower individuals to take control of their Personal Data and to support organisations with their lawful processing of Personal Data. The DPA 2018 was amended on 1st January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

1.3 The UK GDPR is the "UK General Data Protection Regulation". It is a UK law which came into effect on 1st January 2021 and supplements the DPA 2018. It is based on the EU GDPR (General Data Protection Regulation (EU) 2016/679), which applied in the UK before that date, with some changes to make it work more effectively in a UK context. It sets out the key principles, rights and obligations for most processing of Personal Data in the UK, except for law enforcement and intelligence agencies.

1.4 The purpose of this Policy is to set out how the College will comply with the requirements of the UK GDPR and DPA 2018.

2. SCOPE

2.1 This Policy applies to all sites and all users of the College systems, including staff, students, contractors and visitors to the College, and link organisations such as the Wildlife Park, who are permitted access to the College's computing or information resources (including directors and employees of any such organisation).

2.2 This Policy also applies to all Personal Data and Special Categories of Personal Data (previously known as "Sensitive Data") processed (used) by the College and as

defined under the UK GDPR and DPA 2018, including structured sets of Personal Data held in electronic or other filing systems that are accessible according to specified criteria.

2.3 "Personal Data" means any information relating to an identified or identifiable living individual (section 3(2) DPA 2018). "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to:

(a) a unique identifier such as a name, an identification number, location data or an online identifier, for instance, name, postal address, email address, telephone number, etc; or

(b) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

2.4 Special Categories of Personal Data are Personal Data deemed to be more sensitive by law and so need additional protection. The UK GDPR defines "Special Category Data" as:

- Personal Data revealing racial or ethnic origin;
- Personal Data revealing political opinions;
- Personal Data revealing religious or philosophical beliefs;
- Personal Data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

2.5 This does not include Personal Data about criminal allegations, proceedings or convictions, as separate rules apply.

2.6 For Personal Data to be processed lawfully, there must be a lawful basis for any processing, (see section 6). A lawful basis is also required in the event any Personal Data is to be shared.

2.7 Special Category Data cannot be processed unless in addition to a lawful basis for processing there is at least one *further* condition for processing Special Category Data. These further conditions are:

(a) Explicit consent;
(b) Employment, social security and social protection (if authorised by law);
(c) Vital interests;
(d) Not-for-profit bodies;
(e) Made public by the data subject;
(f) Legal claims or judicial acts;
(g) Reasons of substantial public interest (with a basis in law);
(h) Health or social care (with a basis in law);
(i) Public health (with a basis in law);
(j) Archiving, research and statistics (with a basis in law).

2.8 This Policy is supplemented by a number of separate data protection policies and procedures, details of which are at section 15, below.

3. DATA PROTECTION PRINCIPLES

3.1 The UK GDPR sets out seven key principles that should lie at the heart of an organisation's approach to the processing of Personal Data including Special Category Data:

- **lawfulness, fairness and transparency** - telling people why you need their Personal Data and what you intend to do with it, and making sure you have a lawful basis for any processing that you do (see section 6);
- **purpose limitation** – making sure that you only use the Personal Data for what you said you were going to use it for;
- **data minimisation** – not collecting more Personal Data than you need/intend to use, just because it is nice to have;
- **accuracy** - making sure you keep any Personal Data accurate and up to date;
- **storage limitation** – making sure you do not keep any Personal Data for longer than you need;
- **integrity and confidentiality (security)** - putting in place organisational and technical measures to ensure that the Personal Data is kept secure;
- **accountability** - taking responsibility for what you do with Personal Data and how you comply with the other principles.

3.2 The College will ensure it complies with the data protection principles by:

- only processing Personal Data where an appropriate legal basis to do so exists and only in order to meet the College's operational needs or fulfil legal requirements[1];
- being clear with individuals whose Personal Data we process as to how we store it, what we do with it and why;
- taking steps to ensure that Personal Data is up to date and accurate;
- establishing appropriate retention periods for any Personal Data held[2];
- ensuring that Data Subjects' rights (see section 11) can be appropriately exercised including responding to any valid Subject Access Requests promptly and in any event within one month of receiving them (unless limited exceptions apply) (see the College's Subject Access Request Policy for further details, available at https://www.askham-

[1] For further details see the Staff Privacy Notice and Student Privacy Notice available at https://www.askham-bryan.ac.uk/publication-scheme-data-protection/

[2] See the College's Data Retention Policy for further details, available at https://www.askham-bryan.ac.uk/publication-scheme-data-protection/

bryan.ac.uk/publication-scheme-data-protection/);

- regularly reviewing data protection procedures and guidelines within the organisation;
- adopting national data protection best practice, including incorporation of appropriate learning from any published ICO data protection and/or European Data Protection Board (EDPB) guidance;
- ensuring that all staff are made aware of good practice in data protection and providing adequate training for all staff responsible for processing Personal Data;
- appointing a Data Protection Officer who is responsible for data protection compliance and who is a point of contact for all data protection issues (see section 9);
- sharing information where required by law and where approved information/data sharing agreements are in place and when agreed processes have been followed.

4. PRIVACY BY DESIGN AND DEFAULT

4.1 The College will ensure that data protection principles are taken into account throughout the process of designing a new process, product, policy or services, rather than treating it as an afterthought. This means assessing carefully and implementing appropriate technical and organisational measures and procedures from the outset to ensure the processing complies with the law and protects the rights of Data Subjects. This process is known as "privacy by design and default".

5. DATA MINIMISATION

5.1 The College will also ensure mechanisms are in place to ensure that, by default, only Personal Data which are necessary for each specific purpose are processed. This includes ensuring that only the minimum amount of Personal Data is collected and processed for a specific purpose; that the extent of processing is limited to that necessary for each purpose; the Personal Data is stored no longer than necessary, and access is restricted to that necessary for each purpose.

6. LAWFUL BASIS FOR PROCESSING AND SHARING PERSONAL DATA

6.1 Under the UK GDPR and DPA 2018, you must have a lawful basis for processing and or sharing Personal Data with other organisations. Lawful bases permitted by the UK GDPR are:

1. **Consent** of the Data Subject.

   Consent is defined in Article 4(11) UK GDPR as:

   *"any **freely given, specific, informed and unambiguous** indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*

This could include ticking a box ["positive opt in"] when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the Data Subject's acceptance of the proposed processing of their Personal Data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent.

Consent also means giving people genuine ongoing choice and control over how someone's data is used.

Please note: in some circumstances, it may not be appropriate or desirable to rely on consent as the basis for processing, for instance, where the processing is required in order to comply with a legal or statutory obligation (for instance, a safeguarding concern to the Local Authority Designated Officer or "LADO"[3]), and in those circumstances, a Data Subject cannot give or withdraw their consent to that processing.

2. **Performance of a contract** - organisations can rely on performance of a contract if:

   a) they have a contract with someone and need to process their Personal Data to comply with their obligations as part of that contract; or

   b) they do not yet have a contract with someone, but an individual has asked an organisation to do something as an initial step (for example, provide a quote), with a view to possibly entering into a contract with that organisation at a later date and the organisation needs to process the individual's Personal Data to do so.

3. **Legal obligation**, i.e. where the processing is necessary to comply with a common law or statutory obligation (Health and Safety at Work Act 1974, etc).

4. **Vital Interests** - you can collect, use or share Personal Data in emergency situations, to protect someone's life;

5. **Public Task** – where the processing of Personal Data is necessary for public functions and powers that are set out in law, or to perform a specific task in the public interest[4];

6. **Legitimate Interests** – where the processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data (Article 6(1)(f) UK GDPR).

[3] "LADO" stands for Local Authority Designated Officer. This person within a local authority is responsible for overseeing and managing allegations or concerns about individuals who work with or volunteer for children. The LADO ensures these concerns are handled fairly and thoroughly, protecting both the child's welfare and the individual's rights.

[4] Section 8 of the Data Protection Act 2018 (DPA 2018) says that the public task basis will cover processing necessary for:

- the administration of justice;
- parliamentary functions;
- statutory functions;
- governmental functions; or
- activities that support or promote democratic engagement.

However, this is not intended as an exhaustive list.

Legitimate interests is the most flexible of the six lawful bases for processing and could theoretically apply to any type of processing carried out for any reasonable purpose; but organisations cannot assume it will always be the most appropriate. It is likely to be most appropriate where an organisation uses people's Personal Data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing, for instance, to prevent fraud, or for security.

7. WHY THE COLLEGE PROCESSES PERSONAL DATA

7.1 The College needs to process certain information about its employees, students, external contractors, suppliers and other third parties such as visitors to the College, about parents, guardians and carers, etc, for a number of purposes: to meet its legal obligations, in particular to its staff and students, and otherwise fulfill its statutory obligations as an educational institution under the Further and Higher Education Act 1992 and other applicable legislation.

7.2 In the case of staff:

- for the recruitment process and for carrying our pre-employment checks;
- for checking your identity and right to work in the UK;
- for checking your qualifications (which may, if necessary, be shared with awarding organisations);
- for carrying out our role as your employer or potential employer;
- to support and manage employees;
- to gather evidence and any other steps relating to possible grievance or disciplinary matters and associated hearings;
- to enable the development of a comprehensive picture of the workforce and how it is deployed;
- to process payroll, pensions, expenses claims and other financial transactions;
- to make decisions about salary reviews and compensation;
- for conducting performance reviews;
- to maintain the College's accounts and for insurance purposes;
- for dealing with HMRC;
- to allow for better financial modelling and planning;
- to inform the development of recruitment and retention policies;
- for safeguarding students including maintaining the Single Central Register;
- to maintain accident records and to otherwise comply with health and safety legislation;
- for communicating with you and for marketing purposes;
- in the case of use of CCTV, to maintain the security of the College's premises, for preventing and investigating crime and when investigating disciplinary matters, etc (see the College's CCTV Policy for further details);
- to monitor your use of our information and communication systems to ensure compliance with our IT policies;
- to ensure network and information security and preventing malicious software distribution.

7.3 In the case of students:

- to provide education, support student learning and to provide general advice services for students;
- for enrolment purposes, to consider whether to offer places to students and to record and track a student's learning journey, once their application to the College has been successful;
- to maintain learner profiles and records of work for each student;
- to monitor student progress and attainment;
- to arrange student travel or accommodation;
- to provide catering services;
- to organise offsite activities or student work experience;
- for handling student funding and bursaries;
- for safeguarding purposes including maintaining the Single Central Register and to provide appropriate pastoral care;
- to keep students safe (food allergies, or emergency contact details);
- to maintain the College's accounts and for insurance purposes;
- to process financial transactions (payment for offsite activities, accommodation, etc);
- to assist with the collection of monies due to the College;
- to assist City of York Council Electoral Services check the eligibility to vote of students and add such students as are eligible to the electoral register;
- to enable City of York Council Tax department to apply appropriate exemptions and discounts for council tax purposes (if applicable) to qualifying full time students;
- in the case of use of CCTV, to maintain the security of the College's premises, for preventing and investigating crime and when investigating disciplinary matters, etc (see the College's CCTV Policy for further details);
- to maintain accident records and to otherwise comply with health and safety legislation;
- to monitor students' use of our information and communication systems to ensure compliance with our IT policies;
- to ensure network and information security and preventing malicious software distribution;
- to assess the quality of our services and for complaints handling;
- to meet the statutory duties placed upon us for the Department for Education (DfE) data collections.

7.4 For further details, including how the College processes parent, guardian, carer and visitor data, see the Privacy Notice for Parents Carers and Guardians and or the Visitors Privacy Notice, available at https://www.askham-bryan.ac.uk/publication-scheme-data-protection/

8. WHY THE COLLEGE SHARES PERSONAL DATA

8.1 The College is required by law to share some Personal Data and in some cases, Special Category Data, with certain third parties, such as the Department for Education (as a condition of the College's funding), local authorities (who are under an obligation to ensure that young people aged 16 – 18, where possible, do not become NEET, i.e. Not in Education, Employment, or Training), OfS (Office for Students), Ofsted, Student Loans Company, Higher Education Statistics Agency ("HESA"), OIA, and awarding bodies.

8.2 In most cases, the College is under a legal or statutory obligation to share this information.

8.3 The College may also need to share Personal Data and in some cases, Special Category Data, to provide certain non-core services to students, such as transport, catering, offsite activities, etc

8.4 In other instances, the College will only share Personal Data with an individual's consent. That consent can be withdrawn at any time; but withdrawing consent could have implications for the provision of that service.

8.5 Where appropriate, the College will first enter into a Data Sharing Agreement with the organisation receiving that information, to ensure that the rights and freedoms of Data Subjects' affected by the sharing are properly protected.

Safeguarding

8.6 The College has a legal obligation to ensure the safety and wellbeing of its students whilst at the College. This duty is typically referred to as "Safeguarding".

8.7 Essentially it is about keeping children and vulnerable adults safe; looking for signs of possible abuse, neglect, etc, and raising any concerns with the appropriate authorities if those concerns are serious enough, or the College is otherwise required by law to do so.

8.8 Where it is necessary for the purposes of Safeguarding, information about an individual may sometimes be shared with appropriate authorities such as the police and Social Services, without a Data Sharing Agreement first being in place.

8.9 If there is any conflict between the College's obligations under data protection legislation and the College's obligations under Safeguarding, then the obligations under Safeguarding will take precedence.

9. ROLES AND RESPONSIBILITIES

9.1 The College is the Controller under data protection legislation for the Personal Data it processes for its own purposes (as set out at section 7). In some instances, it will be a Controller in common with other organisations, such as the Department for Education ("DfE").

9.2 A "Controller" is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. A "Controller in common" refers to situations where multiple parties independently process the same data; but for different purposes. "A Processor" is a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller and under their authority/express instructions.

Data Protection Officer

9.3 The College's Data Protection Officer is responsible for ensuring compliance with this Policy and the College's other data protection policies and procedures (see section 15), and advising the College generally on matters relating to data protection, and is assisted by the Legal and Compliance Adviser and Head of IT.

9.4 The College's Data Protection Officer is Judith Clapham, Deputy Chief Executive Officer. Judith can be contacted on judith.clapham@askham-bryan.ac.uk . Data protection queries can also be sent to the Legal and Compliance Adviser at jethro.powell@askham-bryan.ac.uk or DataProtection@askham-bryan.ac.uk .

9.5 The Data Protection Officer is also responsible for:

- acting as primary contact on any data protection queries;
- acting as primary contact for Data Subjects and the UK's Supervisory Authority, the ICO ("Information Commissioner's Office");
- approving responses to Subject Access Requests;
- monitoring the completion of mandatory data protection training for all staff (assisted by line managers).

Staff responsibilities

9.6 All staff are responsible for ensuring they comply with this Policy and the College's other data protection policies and procedures (see section 15) and have an obligation to make themselves aware of what those policies and procedures are and familiarise themselves with those.

9.7 All staff will also:

- observe all forms of guidance, codes of practice and procedures, in particular guidance from the ICO, about the collection, sharing, handling and use of Personal Data, that may be issued from time to time via Staff Notices, etc;
- only collect and process information in accordance with the purpose for which it is required to be used by the College to meet its statutory requirements and business needs;
- ensure the information is destroyed when no longer required, in line with the College's Data Retention Policy and Procedure;
- upon receipt of a request by or on behalf of an individual for information held about them (Subject Access Request), immediately refer any such requests to the College's Legal and Compliance Adviser to respond to, as per the College's Subject Access Request Policy and Procedure;
- understand that breaches of this Policy may result in scrutiny by the Information

Commissioner's Office (ICO) with the potential for fines to be levied against the College and accompanying reputational damage;

- ensure they successfully complete their mandatory training.

9.8 For further details on the College's Subject Access Request Policy and Data Retention Policy, please see https://www.askham-bryan.ac.uk/publication-scheme-data-protection/

Staff training

9.9 To ensure all staff understand their obligations and Data Subjects' rights under data protection legislation, in particular under the UK GDPR and the DPA 2018, all staff are required to undertake mandatory annual data protection training and mandatory data protection and Cyber Security training will also form part of the induction process for all new employees.

10. DATA BREACH NOTIFICATION

10.1 A "Data Breach" is defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data". A Data Breach can therefore be accidental or deliberate.

10.2 A Data Breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some Data Breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other Data Breaches can significantly affect individuals whose Personal Data has been compromised.

10.3 Examples of a Data Breach are:

- access by an unauthorised third party (such as a hacker);
- sending Personal Data to an incorrect recipient (perhaps by sending an email to the wrong person or by sending post to the wrong address);
- loss or theft of personal devices (such as a mobile or laptop) containing Personal Data;
- alteration of Personal Data without permission;
- loss of availability of Personal Data; and/or,
- where Personal Data is accessed by someone without the proper authorisation and or that person then passes on that information to someone else.

10.4 A Data Breach is therefore not limited to just loss or theft of Personal Data.

10.5 In the event of a Data Breach, staff must immediately contact the College's Data Protection Officer, Judith Clapham (judith.clapham@askham-bryan.ac.uk), Legal and Compliance Adviser (jethro.powell@askham-bryan.ac.uk) and or the Head of IT (tazambal.Ali@askham-bryan.ac.uk), who will need to investigate the circumstances of the Data Breach and assess the potential damage that could be caused to any affected Data Subject(s), as per the College's Data Breach Reporting Policy and Procedure.

10.6 If the College's Data Protection Officer considers that there is a high risk of the Data Breach adversely affecting Data Subject(s)' rights and freedoms, then the Information Commissioner's Office ("ICO") must also be informed of the Data Breach.

10.7 Overall responsibility for investigating Data Breaches rests with the College's Data Protection Officer who may delegate the investigation or aspects of the investigation to the Head of IT and or Legal and Compliance Adviser, as appropriate.

10.8 Staff involved in the breach will be required to cooperate in that investigation. Failure to cooperate could lead to disciplinary action.

10.9 Please see the College's Data Breach Reporting Policy for further details, at https://www.askham-bryan.ac.uk/publication-scheme-data-protection/

11. SUMMARY OF INDIVIDUALS RIGHTS

11.1 The UK GDPR and DPA 2018 create certain rights for individuals (referred to as "Data Subjects"). Some of these rights existed previously, under the Data Protection Act 1998; but others are new, and some have been expanded upon.

11.2 A Data Subject under the UK GDPR and the Data Protection Act 2018 has the following rights:

1. the right to be **informed** – the right for a Data Subject to be told what Personal Data an organisation processes about them and why and how long that information will be held for before it is anonymised (or pseudononymised) or deleted or destroyed;

2. the right of **access** – a right to submit a request, known as a Subject Access Request, to ask what Personal Data an organisation holds about that individual and to be provided with a copy of that Personal Data (but not necessarily a copy of the document(s) that information is contained in). Unlike under the Data Protection Act 1998, the deadline for responding to such a request is now one month starting the day the request is received (as opposed to 40 days) and no fee is now chargeable for responding to a Subject Access Request;

3. the right to **rectification** – a right to have inaccurate or incomplete Personal Data rectified. In some circumstances, an organisation can refuse a request for rectification, but usually only where the organisation considers the request manifestly unfounded or excessive, taking into account whether the request is repetitive in nature;

4. the right to **erasure** – a right to deletion or removal of Personal Data where there is no compelling reason for its continued processing (although this only applies in certain circumstances; it is not an absolute right);

5. the right to **restrict processing** – a right to limit the way an organisation processes an individual's Personal Data where the individual contests the accuracy of that data or for instance when processing is unlawful and the individual opposes erasure and requests restriction instead. This is not an absolute right, and the organisation is still entitled to *store* that Personal Data;

6. the right to **data portability** – the right of a Data Subject to be given a copy of any Personal Data held by an organisation in a "commonly used and machine-readable" format, so that they can transfer that data to another organisation. This is likely to have limited application here at the College and is usually only available where someone is transferring from one service provider, to another service provider, such as from one utility company to another, and also depends on the legal basis for processing;

7. the right to **object** – the right to object to the processing of an individual's Personal Data, unless the organisation can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual, or the processing is for the establishment, exercise or defence of legal claims;

8. **rights in relation to automated decision making and profiling** – automated decision making and profiling is the process whereby Personal Data is used to evaluate certain personal aspects relating to an individual, such as their work or economic situation, health, personal preferences, interests, etc to assist, for instance, with direct marketing to that individual.

   Automated decision making and profiling is unlikely to apply here at the College and usually applies where pre-programmed algorithms or other criteria are used to make a decision, without human involvement.

   An example would be, you apply for a loan from a bank or building society using the bank or building society's online loan calculator. If you are turned down for that loan, it is because a program or algorithm made that decision, as opposed to an actual human being. As such, you have a right to challenge that decision.

11.2 For further details on how you can exercise your rights under the UK GDPR and DPA 2018, please see the College's Subject Access Request Policy and Data Subject Rights Policy for further details, at https://www.askham-bryan.ac.uk/publication-scheme-data-protection/

12. OVERRIDING OBJECTIVE

12.1 At all times, the rights of the individual are paramount.

12.2 When processing and or sharing any Personal Data, staff must ask themselves, "is the use of this Personal Data in this way consistent with the reasons it came into our possession in the first place?"

12.3 If the answer is in the negative, then staff should stop the processing and seek further advice from either the College's Data Protection Officer or Legal and Compliance Adviser, before processing the Personal Data any further.

13. COMPLAINTS

13.1 If you are not satisfied with how the College has processed your personal data, or are not satisfied with how the College has responded to a request to exercise one or more of your data subject rights, as set out above, you have the right to make a complaint. In the first instance, this should be to the College; but you also then have the right to refer the complaint to the ICO if you are not satisfied with the College's response.

13.2 Please submit full details of your complaint to enquiries@askham.bryan.ac.uk, as per the College's Complaints Policy which is available at https://www.askham-bryan.ac.uk/publication-scheme-customer-services/ Please use the Stage 2 Compliant form which is also available at https://www.askham-bryan.ac.uk/publication-scheme-customer-services/

13.3 In accordance with the College's Complaints Policy, all complaints will be acknowledged within 2 working days, and the College will endeavour to provide a response within 10 working days. If more time is needed to investigate your complaint and provide a response, we will let you know. If you are not satisfied with the College's response to your complaint, you have the right to appeal, and ultimately, the right to complain to the ICO.

Please note: although you may complain to the ICO at any time, the ICO is likely to ask you to exhaust the College's complaints process first, before it processes your complaint. Please see the ICO's website www.ico.org.uk for further details.

13.4 The College is registered with the Information Commissioner's Office ("ICO"). The Registration Number is Z6170811. Renewal of the registration takes place annually on 22 January.

14. MONITORING AND REVIEW

14.1 The Deputy Chief Executive Officer will maintain oversight of the effectiveness of these arrangements.

14.2 This policy and the implementation arrangements which underpin it will be reviewed annually by the Deputy Chief Executive Officer and Legal and Compliance Adviser.

15. SUPPORTING/RELATED DOCUMENTS

15.1 This policy is supplemented by the following policies and procedures which should be referred to if and when the situation arises:

Subject Access Request Policy
Subject Access Request Procedure (internal use only)
Data Sharing Policy
Data Sharing Procedure (internal use only)
Data Retention Policy
Data Retention Procedure (internal use only)
Data Breach Reporting Policy

Data Breach Reporting Procedure (internal use only)
Data Subject Rights Policy
Data Subject Rights Procedure (internal use only)
CCTV Policy
CCTV Procedure (internal use only)
Privacy and Electronic Communications Regulations Policy
Information Security Policy
Online Safety Policy
Online Safety Procedure (internal use only)
Data Classification Policy (internal use only)
Data Privacy Impact Assessment Guidance (internal use only)
Key Partners and Suppliers (Data Protection Compliance) (internal use only)
Bring Your Own Device Policy (internal use only)
Clear Desk and Clear Screen Policy (internal use only)
Staff Privacy Notice
Student Privacy Notice
Visitors Privacy Notice
Student Recruitment and Marketing Privacy Notice
Privacy Notice for Parents Carers and Guardians
Access to IT Systems (Starters and Leavers) Procedures

16. RELEVANT LEGISLATION

16.1 In all aspects of this policy the College will comply with the following legislation:

Data Protection Act 2018
UK General Data Protection Regulation
Privacy and Electronic Communications Regulations 2003
Codes of Practice of the Information Commissioner's Office
Human Rights Act 1998
Equality Act 2010

17. DOCUMENT HISTORY

Date of Issue: 21st July 2025 and 12th June 2026 (update to section 13)
Approved on: 24th June 2025
Next review: June 2026
SLT Owner: Deputy Chief Executive Officer
Author: Legal and Compliance Adviser
Publication requirements: PUBLIC