ASKHAM BRYAN COLLEGE

Data Protection Policy
GA23

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. WHY THE COLLEGE PROCESSES PERSONAL DATA

1.1. The College needs to process certain information about its employees, students, external contractors, suppliers and other third parties ("Personal Data") for a number of purposes, such as, but not limited to the following:

a) providing education, support and general advice services for students and facilities for clients;

b) for enrolment purposes and to record and track a student's learning journey, once their application to the College has been successful;

c) to maintain Learner Profiles and records of work for each student;

d) arranging student travel or accommodation;

e) providing catering services;

f) organising offsite activities or student work experience and organising conferences at the College;

g) handling student funding and bursaries and for safeguarding purposes;

h) promoting the College and its services (marketing, promotional materials, photographs of students around campus, etc);

i) for insurance purposes;

j) processing of financial transactions (payment for offsite activities, accommodation, etc);

k) processing of payroll, invoicing and for administrative reasons, in respect of the functioning and governance of the College and College properties, including recruitment and provision of staff contracts;

l) supporting and managing employees;

m) collection of monies due to the College;

n) use of CCTV to maintain the security of the College's premises and for preventing and investigating crime;

o) to maintain a register of the College's interests;

p) to maintain accident records and to otherwise comply with health and safety legislation;

q) complaints handling;

r) and to otherwise fulfill its statutory obligations as an educational institution under the Further and Higher Education Act 1992 and other applicable legislation.

1.2. To comply with data protection legislation, in particular the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018, which together replace the Data Protection Act 1998, the College will ensure that all Personal Data that it processes is collected and used fairly, stored securely and not disclosed to any third party unlawfully.

1.3. The College will therefore ensure that any Personal Data it processes (uses) shall be:

a) processed lawfully, fairly and in a transparent manner;

b) collected for specified, explicit and legitimate purposes only and not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which that Personal Data is processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of Data Subjects (a "Data Subject" is a natural, identifiable person) for no longer than is necessary for the purposes for which the Personal Data is processed; and

f) processed in a manner that ensures appropriate security of the Personal Data, including protections against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.4. This Policy applies to anybody who handles Personal Data or other confidential information held by the College, including but not limited to:

a) employees, students and honorary employees of the College;

b) link organisations on campus who are permitted access to the College and/or the College's computing or information resources (including directors and employees of any such organisation); and

c) contractors and suppliers providing a service to the College where they are required to have access to College information and/or the College's computing and network facilities (including any directors and employees of any such contractor or supplier).

Sharing Personal Data

1.5. In some circumstances, the College may agree that it is in an individual's or the College's interests to share Personal Data with a third party, such as a tour operator to be able to provide an offsite activity, or to catering companies, to be able to provide catering facilities (canteen) at the College, and with exam bodies, etc provided appropriate security measures to safeguard that Personal Data against loss or theft or unauthorised access are in place, which in some instances, where we are not under a statutory or legal obligation to share this information, must be subject to an appropriate Data Sharing Agreement.

1.6. The College, all Data Processors and all others who process or use any Personal Data (including but not limited to students and service users) must ensure that they follow the above principles at all times.

Controllers and Processors

1.7. "A Processor" is the party or organisation responsible for processing Personal Data on behalf of a Controller usually on a Controller's instructions.

1.8. A "Controller" determines the purposes and means of processing Personal Data.

1.9. At all material times, the College will be a Controller; but in some instances, depending on the nature of the processing, the College may also be a "Controller in Common" with the other organisation, where each organisation determines the nature of the processing, or a "Processor" where the nature of the processing is determined by the other organisation.

1.10. In some circumstances, the Education and Skills Funding Agency ("ESFA") will also be a Controller for the purposes of GDPR and data protection legislation as will the Department for Education ("DfE").

2. SUMMARY OF INDIVIDUALS RIGHTS

GDPR and the Data Protection Act 2018 expand on a Data Subject's existing rights under the Data Protection Act 1998. A Data Subject under GDPR and the Data Protection Act 2018 now has the following rights:

1. the right to be **informed** – the right 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 information an organisation holds about that individual and to be provided with a copy of that information. Unlike under the Data Protection Act 1998, the deadline for responding to such a request is now one month starting the day after the request (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 (although 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)(see below for further);

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 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, such as a utility company, to another and also depends on the legal basis for processing (see below for further);

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 is unlikely to apply here at the College and usually applies where decisions are made without human involvement, such as whether someone qualifies for a loan which they have applied for online or a recruitment aptitude test which uses pre-programmed algorithms and criteria.

In addition, individuals still have the right (as they did before under the Data Protection Act 1998) to lodge a complaint with the UK's Supervisory Authority, the Information Commissioner's Office (or "ICO" for short) and also the right to compensation for a breach by an organisation of an individual's data protection rights, and for distress.

Where a person wishes to make a complaint to the ICO, they will be expected to have first exhausted an organisation's internal complaints procedure.

3. LAWFUL BASIS FOR PROCESSING AND SHARING PERSONAL DATA

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

1. **Consent** of the Data Subject. Genuine consent is defined as "…any **freely given, specific, informed and unambiguous** indication of the Data Subject's agreement to the processing of Personal Data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.

   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 his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent."

   In some circumstances, where the processing is required in order to comply with a legal or statutory obligation (for instance, reporting requirements to the ESFA or DfE), consent, as a basis of processing, may not apply, and a data subject cannot give or withdraw their consent to that processing.

2. **Performance of a contract**, where the processing is necessary to deliver a contractual service to the Data Subject, for instance, so that the College can perform its obligations under a contract it has with the Data Subject, or because the Data Subject has asked an organisation to do something before entering into a contract (eg provide a quote);

3. **Legal obligation**, ie where the processing is necessary to comply with a common law or statutory obligation (Health and Safety at Work Act 1974, Further and Higher Education Act 1992, etc);

4. Where the processing or sharing of Personal Data is necessary in the Data Subject's "**vital interests**", ie in the event of an emergency and it is not possible to obtain the Data Subject's consent, where they may be injured and unable to give consent. If you can reasonably protect the person's vital interests in another less intrusive way, however, this basis will not apply;

5. **Public task** – where it is necessary to process Personal Data 'in the exercise of official authority' (this covers public functions and powers that are set out in law) or to perform a specific task in the public interest that is set out in law. It is most relevant to public authorities; but it can apply to any organisation that exercises official authority or carries out tasks in the public interest. You do not need a specific statutory power to process personal data, but your underlying task, function or power must have a clear basis in law; and/or

6. **Legitimate interests**, ie where it is in the organisation's or someone else's interests (such as the data subject's) to process and or share information. Legitimate interests is the most flexible lawful basis for processing; but you cannot assume it will always be the most appropriate. It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

4. TYPES OF PERSONAL DATA

Special Category Data

4.1 Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.

4.2 Information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation

is Special Category Data.

4.3 Processing of Special Category Data of personal data is necessary for the performance and discharge of the College's contractual obligations to staff (contract of employment) and to students, ie provision of education and to comply with legal and statutory requirements relating to that provision, and in order for the College to be able to carry out a task in the public interest (provision of education), in accordance with Articles 6 and 9 GDPR and section 10 and Schedule 1, Part 1 of the Data Protection Act 2018, specifically paragraph 8(1) of Schedule 1, Part 1 (equality of opportunity and treatment), paragraph 16 (support for individuals with a particular disability or medical condition), paragraph 17 (counselling), paragraph 18 (safeguarding of children and of individuals at risk) and paragraph 20 (insurance).

Criminal Offence Data

4.4 Processing of Criminal Offence Data is necessary for the performance and discharge of the College's contractual obligations to staff and students and to comply with legal and statutory requirements relating to that provision (including safeguarding),and in order for the College to be able to carry out a task in the public interest (provision of education), in accordance with Articles 6 and 10 GDPR and section 10 and Schedule 1, Part 1 of the Data Protection Act 2018, specifically paragraph 18 (safeguarding of children and of individuals at risk) and paragraph 29 of Schedule 1, Part 1 (consent).

5. OVERRIDING OBJECTIVE

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

5.2 When processing and or sharing any Personal Data, the question must be asked, "is the use of this Personal Data in this way consistent with the reasons it came into our possession in the first place?"

5.3 If the answer is in the negative, you should stop processing and or sharing the Personal Data any further and should speak to College's Data Protection Officer and or Legal and Compliance Adviser and seek further advice.

6. STAFF TRAINING

6.1 To ensure all staff understand their obligations and data subjects rights under data protection legislation, in particular under the GDPR and under the Data Protection Act 2018, all staff will be required to undertake mandatory annual data protection training and data protection training will form part of the induction process for all new employees.

7. DATA PROTECTION OFFICER

7.1. The College Senior Leadership Team has overall responsibility for ensuring compliance with data protection legislation and its associated policies and procedures and has appointed a Data Protection Officer, who is the Clerk to the Corporation.

7.2. The Data Protection Officer will lead on the College's overall approach to data protection, assisted by the Legal and Compliance Adviser.

7.3. In addition, the College's Data Protection Officer, assisted by the Legal and Compliance Adviser, will monitor internal compliance with GDPR and the Data Protection Act 2018, and provide advice on data protection issues and how it impacts the College and its activities, and act as a contact point for Data Subjects and the supervisory authority, the ICO.

7.4. Any person who considers that any of the College's data protection policies and or procedures have not been followed should raise the matter with the College's Data Protection Officer by contacting judith.clapham@askham-bryan.ac.uk or by emailing DataProtection@askham-bryan.ac.uk or by contacting the Legal and Compliance Adviser at jethro.powell@askham-bryan.ac.uk .

7.5. If an individual makes a complaint to the College's Data Protection Officer and is not satisfied with the College's response, he/she may then wish contact the Information Commissioner's Office (or "ICO"), the UK's supervisory authority, at https://ico.org.uk/concerns/ and make a formal complaint. 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.

7.6. Please note that the ICO is unlikely to investigate a complaint without an individual first having made a complaint to the College and exhausting the College's own internal complaints procedure first, before referring the matter to the ICO.

8. RELATED POLICIES AND PROCEDURES

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

GA24 Subject Access Request Policy
GA25 Subject Access Request Procedure (internal use only)
GA26 Data Sharing Policy
GA27 Data Sharing Procedure (internal use only)
GA28 Data Retention Policy
GA29 Data Retention Procedure (internal use only)
GA30 Breach Detection and Reporting Policy
GA31 Breach Detection and Reporting Procedure (internal use only)
GA32 Data Subject Rights Policy
GA33 Data Subject Rights Procedure (internal use only)