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. INTRODUCTION

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 providing education, monitoring performance, tracking attendance and achievements, health and safety, etc.

1.2. The College also processes Personal Data in order to recruit, employ and pay staff, organise courses and comply with its legal obligations to funding bodies (such as the Education and Skills Funding Agency) and the Government.

1.3. 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.

1.4. The College will ensure that Personal Data 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;
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.

1.5. 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).

1.6. Personal Data is processed by the College for many reasons, including, 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) publication of the College magazine;

j) maintaining the College's accounts and for insurance purposes;

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

l) supporting and managing employees;

m) 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;

n) collection of monies due to the College;

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

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

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

r) complaints handling;

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

1.7. 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.

1.8. 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. "A Processor" is the party or organisation responsible for processing Personal Data on behalf of a Controller usually on a Controller's instructions. 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. The Department for Education ("DfE") is the ultimate Controller for the purposes of GDPR and data protection legislation.

2. DATA PROTECTION OFFICER

2.1. The College Senior Management Team has overall responsibility for ensuring compliance with GDPR and data protection legislation and associated policies and procedures and has appointed a Data Protection Officer, who is the Clerk to the Corporation. The Data Protection Officer will lead on the College's overall approach to data protection, assisted, where necessary, by the Legal and Compliance Adviser.

2.2. Any person who considers that this policy has 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.

2.3. If you are not satisfied with the response, you may then wish contact the Information Commissioner's Office at https://ico.org.uk/concerns/. 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.

3. 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 destroyed;

2. the right of **access** – a right to submit a request, known as a Subject Access Request, and to be provided with a copy of all Personal Data held by the organisation about them. Unlike under the Data Protection Act 1998, the deadline for responding to such a request is now 30 days (as opposed to 40 days) and no fee is chargeable for responding to a Subject Access Request;

3. the right to **rectification** – a right to have inaccurate or incomplete Personal Data rectified;

4. the right to **erasure** – a right to deletion or removal of Personal Data where there is no compelling reason for its continued processing;

5. the right to **restrict processing** – a right to have an organisation stop processing 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. The organisation is still entitled to store that Personal Data, however;

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.

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.

9. **right to lodge a complaint** with a Supervising Authority. The UK's Supervisory Authority is the Information Commissioner's Office or "ICO"**;**

10. **right to effective judicial remedy against the Supervising Authority** where an individual feels that the Supervising Authority's decision is incorrect or unfair;

11. **right to effective judicial remedy against the Controller or Data Processor** – the right to institute Court proceedings or judicial review where the organisation concerned is a public body;

12. **right to compensation** – for instance, in respect of a Data Breach (loss or theft or unauthorised access to an individual's Personal Data), a breach by an organisation of an individual's data protection rights, and for distress.

Only 1. – 8. will be the subject of any College policies and procedures; but all of a Data Subject's rights under GDPR and the Data Protection Act 2018 will be respected by the College.

4. 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:

- the **consent of the Data Subject**, although in some instances, Personal Data may need to be processed and can be shared without an individual's consent. Genuine consent requires a positive opt in and is defined as "…any **freely given, specific, informed and unambiguous** indication of the Data Subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her";

- **performance of a contract** (that the College has entered into with the Data Subject or vice versa);

- to ensure that the College complies with a **legal obligation**, such as obligation under statute;

- where the processing or sharing of Personal Data is 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;

- performance of a **public task** or function; and/or

- where it is in the organisation's **legitimate interests** to process and or share information.

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.

Different rights also apply depending on what basis you use:

Legal basis for processing/sharing	Right to erasure	Right to portability	Right to object
Consent	YES	YES	NO (but right to withdraw consent)
Performance of a contract	YES	YES	NO
Legal obligation	NO	NO	NO
"Vital interests"	YES	NO	NO
Public task	NO	NO	YES
Legitimate interests	YES	NO	YES

For further information, please go to the website of the Office of the Information Commissioner ("ICO") https://ico.org.uk/your-data-matters/

5. OVERRIDING OBJECTIVE

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

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?"

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. 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)