ASKHAM BRYAN COLLEGE

Data Breach Reporting Policy 2025 - 2026

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. WHAT IS A DATA BREACH?

1.1 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".

1.2 A Data Breach can have a range of adverse effects on individuals (also known as "Data Subjects"), 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. Examples of a Data Breach are:

- access by an unauthorised third party (such as a hacker);
- deliberate or accidental action (or inaction) by a Controller or Processor;
- 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.

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

What to do in the event of a Data Breach

Staff should immediately report any Data Breach to the College's Data Protection Officer, Judith Clapham (judith.clapham@askham-bryan.ac.uk) and the Legal and Compliance Adviser (jethro.powell@askham-bryan.ac.uk).

2. COLLEGE POLICY IN RESPONSE TO A DATA BREACH

2.1 In the event of a Data Breach, the College's Data Protection Officer, assisted by the Legal and Compliance Adviser and Head of IT, will investigate the circumstances of the Data Breach and assess the potential damage that could be caused to any Data Subjects as a result of the Data Breach. In some cases, this will involve advising any Data Subjects affected by the Data Breach that a Data Breach has happened.

2.2 If the College's Data Protection Officer considers the breach to be sufficiently serious, i.e. there is a high risk of the Data Breach adversely affecting a Data Subject's rights and freedoms, then the Data Protection Officer will complete the ICO's self-assessment questionnaire, and if appropriate, the Information Commissioner's Office ("ICO") will also be informed of the Data Breach.

2.3 Overall responsibility for investigating a serious data breach rests with the Data Protection Officer who may delegate the investigation or aspects of the investigation to the Head of IT and or Legal and Compliance Adviser. Less serious breaches may be investigated by the Legal and Compliance Adviser and or Head of IT, as appropriate, however, the College's Data Protection Officer will be notified.

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

3. SCOPE

3.1 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 the College's computing or information resources (including directors and employees of any such organisation).

4. RESPONSIBILITIES

4.1 The College's Data Protection Officer, assisted by the Legal and Compliance Adviser and Head of IT, will respond to and investigate all Data Breaches and or near misses. The College's Data Protection Officer, Legal and Compliance Adviser and Head of IT, assisted by others where necessary, will assume principal responsibility for any management of the College's response to a Data Breach, depending on the nature and extent of that breach.

4.2 The College's Data Protection Officer – and only the College's Data Protection Officer – will be responsible for reporting all reportable breaches to the ICO, in accordance with the College's Data Breach Reporting Procedure.

4.3 All staff will be responsible for reporting all Data Breaches, confirmed or suspected, including any near misses, to the College's Data Protection Officer, Head of IT and or Legal and Compliance Adviser.

4.4 The Legal and Compliance Adviser will maintain a log of all Data Breaches and or near misses.

5. WHAT TO DO IN THE EVENT OF A DATA BREACH

5.1 In the event of a Data Breach as defined above, the matter should be reported immediately to the College's Data Protection Officer by contacting judith.clapham@askham-bryan.ac.uk, to the Head of IT by contacting tazambal.ali@askham-bryan.ac.uk and to the Legal and Compliance Adviser by contacting jethro.powell@askham-bryan.ac.uk or by emailing DataProtection@askham-bryan.ac.uk). Alternatively, the above can be contacted on Teams.

5.2 Staff who receive an email they consider suspicious should inform IT immediately and only forward the email to IT to investigate further, if asked to do so by IT.

5.3 Where appropriate, the Data Breach will be reported to the ICO within 72 hours of the breach occurring. See below for further details.

6. INVESTIGATION

Significant Data Breach

6.1 In the event of a significant Data Breach, the College's Data Protection Officer, in conjunction with the Legal and Compliance Adviser and Head of IT, will:

- **investigate** the Data Breach;
- **assess** the likely impact of the Data Breach;
- **seek to contain** and where possible, **limit the scope** of the Data Breach;
- if any Personal Data has been lost, **seek to recover** that data;
- **notify** any affected Data Subjects, if appropriate to do so;
- and consider **what lessons can be learned,** either following an internal investigation into the incident, and or further to recommendations by the ICO, to avoid a similar Data Breach happening again. Where necessary, staff will be provided with further training.

6.2 Where there is a high or significant risk that the Data Breach will adversely affect Data Subjects' rights and freedoms, then the Principal and Chief Executive will also be notified of the Data Breach and the College's Data Protection Officer will coordinate their response to the Data Breach with the Principal and Chief Executive.

Less serious breaches

6.3 As stated above, less serious Data Breaches may be investigated by the Legal and Compliance Adviser and or Head of IT, as appropriate, however, the College's Data Protection Officer will be notified.

Data Breach Log

6.4 The Legal and Compliance Adviser will maintain a log of all Data Breaches.

See the Data Breach Reporting Procedure for further details.

7. INFORMING THE ICO

7.1 The College's Data Protection Officer will be responsible for informing the UK's Supervisory Authority, the Information Commissioners Office ("ICO"), of any Data Breach and the College will consider any guidance from the ICO when responding to the breach. **No other member of staff should contact the ICO, without the express permission of the Data Protection Officer.**

7.2 Please note: not every Data Breach must be reported to the ICO; only breaches where there is a high risk of the Data Breach adversely affecting Data Subjects' rights and freedoms, in which case, the Data Breach must be reported to the ICO within 72 hours of the breach occurring.

7.3 Even if the College ultimately decides not to advise the ICO of the Data Breach, the Data Breach should still be logged.

7.4 Where there is a high risk of the Data Breach adversely Data Subjects' rights and freedoms, then the Data Subjects concerned will also be notified of the Data Breach. See the Data Breach Reporting Procedure for further details.

8. DATA PROTECTION OFFICER

8.1 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 and Director of Governance.

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

8.3 In addition, the College's Data Protection Officer, assisted by the Legal and Compliance Adviser and Head of IT, will monitor internal compliance with the UK 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.

8.4 However, all users of College systems, i.e. staff, students, contractors and visitors to the College, and link organisations such as the Wildlife Park, are expected to comply with data protection legislation and support the College's Data Protection Officer, Legal and Compliance Adviser and Head of IT in meeting the College's obligations under data protection legislation, and cooperate with them in the event of a Data Breach or Cyber Security incident.

9. COMPLAINTS

9.1 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.

9.2 Alternatively, they may wish to make a formal complaint. Details of the College's Complaints Policy are available on the College's website (https://www.askham-bryan.ac.uk/publication-scheme-customer-services/) and or on request.

9.3 If an individual makes a complaint to the College and is not satisfied with the College's response, they 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.

9.4 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.

10. MONITORING AND REVIEW

10.1 The Director of Governance will maintain oversight of the effectiveness of these arrangements.

10.2 This policy and the implementation arrangements which underpin it will be reviewed annually by the Director of Governance and Legal and Compliance Adviser.

11. SUPPORTING/RELATED DOCUMENTS

This policy is supplemented by the following policies and procedures:

Data Protection Policy
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 Procedure (internal use only)
Data Subject Rights Policy
Data Subject Rights Procedure (internal use only)

12. RELEVANT LEGISLATION

Data Protection Act 2018
UK GDPR

13. DOCUMENT HISTORY

Date of Issue: 21st July 2025
Approved on: 24th June 2025
Next review: June 2026
SLT Owner: Director of Governance
Author: Legal and Compliance Adviser
Publication requirements: PUBLIC