Data Breach Reporting Policy
2021 - 2022

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. A "Data Breach" is defined as "a breach of security leading to 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, 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.

1.3. 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.

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

1.5. In the event of a Data Breach, the College's Data Protection Officer, Legal and Compliance Adviser and Head of IT will need to investigate the circumstances of the Data Breach and assess the potential damage that could be caused to an individual(s) (or Data Subject(s)) as a result of the Data Breach.

*a "Controller" is defined as the person or organisation that determines the purposes and means of processing Personal Data and a "Processor" is defined as the person or organisation responsible for processing Personal Data on behalf of a Controller

1.6. In some cases, this will involve advising the individual(s) affected by the Data Breach that a Data Breach has happened.

1.7. 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 Data Subject(s)' rights and freedoms, then the Information Commissioner's Office ("ICO") must also be informed of the Data Breach.

1.8 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.

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

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 and the Rural Business Research Unit ("RBRU"), who are permitted access to the College and/or the College's computing or information resources (including directors and employees of any such organisation).

3. WHAT TO DO IN THE EVENT OF A PERSONAL DATA BREACH

3.1 In the event of a Data Breach, staff should report the incident immediately to the College's Data Protection Officer by contacting judith.clapham@askham-bryan.ac.uk (please also cc the Legal and Compliance Adviser at jethro.powell@askham-bryan.ac.uk) or by emailing DataProtection@askham-bryan.ac.uk).

Virus attack, hacking attempt, document sent in the post to the wrong address, etc

3.2 In the event of a Data Breach which could be as a result of opening a file with a virus, staff **should immediately contact the IT department** so that they can take steps to prevent the hacker getting access to College systems.

3.3 Staff should also report the incident immediately to the College's Data Protection Officer by contacting judith.clapham@askham-bryan.ac.uk (please also cc the Legal and Compliance Adviser at jethro.powell@askham-bryan.ac.uk) or by emailing DataProtection@askham-bryan.ac.uk).

4. INVESTIGATION

4.1 The College's Data Protection Officer in conjunction with the Legal and Compliance Adviser and Head of IT will then:

- **investigate** the Data Breach – how did it happen? When did it happen? How much Personal Data has been lost, corrupted, etc? Does this contain any Special Category Data? And what is the likely impact of this Data Breach going to be on the Data Subject(s) concerned?;
- **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;
- **assess** the likely impact of the Data Breach;
- **notify** any affected Data Subjects, if appropriate to do so;
- **evaluate** the situation;
- 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 and advise staff accordingly, so that information can be disseminated throughout the organisation. Where necessary, staff will be provided with further training.

4.2 In the event of a **serious breach**, i.e. where there is a **high or significant risk that the Data Breach will adversely affect individuals' rights and freedoms**, then the College's Chief Executive Officer 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 College's Chief Executive Officer.

4.3 The College's Data Protection Officer will also be responsible for informing the UK's Supervisory Authority, the Information Commissioners Office ("ICO") of any Data Breach.

4.4 Not every Data Breach must be reported to the ICO; **only breaches where there is a high risk of the Data Breach adversely affecting individuals' rights and freedoms**, in which case, the Data Breach must be reported to the ICO within 72 hours of the breach occurring.

4.5 **Where there is a high risk of the Data Breach adversely affecting an individual's or individuals' rights and freedoms, then the Data Subject(s) concerned must also be notified of the Data Breach.**

4.6 No 2 Data Breaches are likely to be the same. Each Data Breach should therefore be assessed on a case by case basis.

4.7 Even if the College ultimately decides not to advise the ICO of the Data Breach, the Data Breach should still be documented, in the event the College has to justify that decision later.

4.8 Failure to notify the ICO of a Data Breach and or put in place an effective remedy on discovery of a Data Breach is likely to result in enforcement action by the ICO, which could include a fine. The maximum fine is presently £17,500,000 (previously €20 million) or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher, depending on the nature and extent of the breach.

Data Breach by Data Processors, etc.

4.9 Any Processors used by the College should be provided with a copy of the College's Data Sharing Policy and they will be made aware that in the event of a Data Breach by them, that they will inform the College immediately of the breach.

4.10 Where the College acts as the Processor, then it will inform the third party organisation that acts as Controller immediately of any Data Breach so that that third party organisation can take appropriate action to remedy the breach.

4.11 "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. Two or more Controllers that each determine how they process Personal Data are known as "Controllers in Common".

5. DATA PROTECTION OFFICER

5.1. 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.

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

5.3. 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.

5.4. **However, all users of College systems, ie staff, students, contractors and visitors to the College, and link organisations such as the Wildlife Park and the Rural Business Research Unit ("RBRU"), 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.**

5.5. 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 .

5.6. 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.

5.7. 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.

5.8. **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.**

6. RELATED POLICIES AND PROCEDURES

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)
Breach Detection and Reporting Procedure (internal use only)
Data Subject Rights Policy
Data Subject Rights Procedure (internal use only)