ASKHAM BRYAN COLLEGE

Data Breach Reporting Policy
GA30

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. "Personal Data" is defined as "any information relating to an identifiable natural person who can be directly or indirectly identified in particular by reference to an identifier".

1.3. "Directly identifiable Personal Data" refers to names, student numbers, National Insurance numbers, etc.; unique identifiers from which it is possible to work out a person's identity because these numbers or that data are linked to that one individual only.

1.4. "Indirectly identifiable Personal Data" would be separate data that can be pieced together to identify an individual. For instance, a *combination of separate data about gender, age, and position within an organisation and or salary may well enable you to identify a particular individual, even though that person may not be referred to by name.*

1.5. Examples of a Data Breach are:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a Controller or Processor; 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;
- sending Personal Data to an incorrect recipient;
- computing devices containing Personal Data being lost or stolen;
- alternation 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.

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

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

Email sent to the wrong recipient

2.1 In the event of a Data Breach which involves accidentally sending Personal Data to the incorrect recipient, staff should seek to **immediately recall that email(s**) and then **also contact the recipient(s)** (either by telephone or email**)(by telephone if they fail to respond to the email) to ask them to confirm that they have deleted that email** as in some cases, a recall can be unsuccessful and the message may still be visible, despite the recall.

2.2 Staff will need to be persistent and continue to contact recipient(s) of such emails until all such recipient(s) have confirmed deletion. If the email was inadvertently sent to the wrong group, then every member of the group must be contacted.

2.3 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 so that they can advise if any further action is necessary.

Virus attack, hacking attempt, etc

2.4 In the event of a Data Breach which could be as a result of opening a file with a virus, inputting your personal details and password in response to an email you have received that you then discover is not genuine, etc you should immediately contact the IT department so that they can take steps to prevent the hacker getting access.

2.5 You should also advise the College's Data Protection Officer (by contacting judith.clapham@askham-bryan.ac.uk or by emailing DataProtection@askham-bryan.ac.uk) as well as the College's Legal and Compliance Adviser (jethro.powell@askham-bryan.ac.uk) and Head of IT (declan.whelan@askham-bryan.ac.uk) so that they are also aware of the situation.

2.6 The College's Data Protection Officer in conjunction with the Head of IT and Legal and Compliance Adviser will then decide on what is an appropriate course of action for the College to take in light of the nature and extent of the Data Breach, including whether or not to report the matter to the ICO. **Staff should not undertake to contact the ICO themselves.**

2.7 The College's Data Protection Officer in conjunction with other appropriate personnel as required will:

- **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** to avoid a similar Data Breach happening again and advise staff accordingly, so that information can be disseminated throughout the organisation.

2.8 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.

2.9 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, subject to the Chief Executive's approval.

2.10 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.

2.11 **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.**

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

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

2.14 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 €20 million (approximately £17 million) or 4% of annual turnover.

Data Breach by Data Processors, etc.

2.15 Any Processors used by the College will 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.

2.16 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.

2.17 "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".

3. DATA PROTECTION OFFICER

3.1 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.

3.2 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.

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

3.4 However, all staff will be 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.

3.5 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 .

3.6 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. 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.

3.7 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.

4. RELATED POLICIES AND PROCEDURES

This policy is supplemented by the following policies and procedures:

GA23 Data Protection Policy
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)
GA31 Breach Detection and Reporting Procedure (internal use only)
GA32 Data Subject Rights Policy
GA33 Data Subject Rights Procedure (internal use only)