



GDPR Data Breach Guidelines

Start Date:	Autumn 2021
Date of Next Review:	Autumn 2024
Author:	Ms J Howard
Responsible Committee:	Finance & Resources Committee

What is a personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Examples of a data breach include, but are not limited to:

- access by an unauthorised third party
- deliberate or accidental action or inaction by a data controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- the loss of availability of personal data

Reporting a breach

When a personal data breach has occurred, the school needs to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then the school must notify the Information Commissioner's Office (ICO); if it's unlikely then you don't have to report it. In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals.

All breaches need to be recorded. If the school decides it does not need to report the breach, it needs to be able to justify this decision.

GDPR places a duty on all organisations to report a notifiable breach to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of it.

A breach notification

When reporting a breach GDPR states that the following information should be provided:

- a description of the nature of the personal data breach including, where possible:
 - the categories and approximate number of individuals concerned
 - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

If all the information required is not available, then an initial report should be made and a follow up full report made without undue delay.

Data Processors

Where the organisation uses a data processor and the processor suffers a breach they should inform the school without undue delay as soon as they become aware of the breach. This requirement allows the school to take steps to address the breach and meet our breach-reporting obligations under the GDPR

Data Breach in school holidays.

The entire school is closed for the Christmas holiday, otherwise during the school holidays there are limited staff on site. If a Data Breach occurs, they will:

- address the breach as far as possible
- notify the ICO of the breach, if necessary
- inform staff not present of the breach on their return to take further action, if necessary

To report a data breach

Personal Data breach helpline 0303 123 1113. Open Mon – Fri 09:00 – 17: 00.

More information about reporting a data breach can be found by following the link below. There is also an online form available for reporting a data breach.

<https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/>

If a data breach occurs at Haileybury Turnford then the Data Breach Form needs to be completed for our records.

Haileybury Turnford

Data Breach Record

Page 1

Data of data breach	
Person dealing with the data breach	
What data bases are involved	
Data type involved	

Breach reported by											
Date/Time reported											
Breach Risk Level		<table border="1"> <tr> <td colspan="2">High</td> </tr> <tr> <td>Medium</td> <td></td> </tr> <tr> <td>Low</td> <td></td> </tr> <tr> <td>None (error report)</td> <td></td> </tr> </table>		High		Medium		Low		None (error report)	
High											
Medium											
Low											
None (error report)											
Reported to DPO		Date/Time:									
Reported to ICO		Date/Time:									
Actions taken											
Preventative action suggestions (including training)											
Notes											
Actions approved by		Date:									

Data Breach Record

Page 2

The Information Commissioner's Office will require the following information

What happened	
---------------	--

When and how the school found out about the breach	
Who has been or might be affected by the breach	100 parents/carers of Y11 students
What actions are being taken as a result of the breach	
Who has been told about the breach	
Who the ICO should contact if they require more information about the breach	

Please also attach any supporting information relating to the breach; emails, letters, documents etc