Name of Policy:	Data Breach Policy
Author:	Katie Findlater
Applicable to:	Staff (including Employees, Governors, Trustees, and Volunteers), Data Processors, and Third Parties
Effective date:	28/10/2026
Date of next review:	27/10/2027

Version History Log

Version	Description of Change	Date of Policy Release
1.0	Original BRIT School Data Breach Policy.	17/01/2025
2.0	Updated to align with Judicium Master Template v10 (Added Document Owner & Approval block, Version History Log, updated DPO contact details, enhanced containment & recovery procedures, detailed factors on data subject harm, signpost to data protection complaints procedure, and Appendix 1 - Data Breach Report Form).	28/10/2026

Data Breach Policy

The UK General Data Protection Regulation (UK GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The UK GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach of the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

Definitions

Personal Data	Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual or an opinion about that person's actions or behaviour.
Special Category Data	Refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data, and personal data relating to criminal offences and convictions.
Personal Data Breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or

	access to personal data or special category data transmitted, stored or otherwise processed.
Data Subject	Person to whom the personal data relates.
ICO	The Information Commissioner's Office, the UK's independent regulator for data protection and information.
Data Protection Officer (DPO)	The person we appoint from time to time to lead the development and implementation of our data protection strategy and compliance with the UK GDPR and other applicable laws.

Responsibility

Katie Findlater has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In their absence, please contact the Headteacher or Senior Leadership Team.

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact Katie Findlater in the first instance if you have any questions about the operation of this policy or the UK GDPR or if you have any concerns that this policy is not being followed. Should the matter remain unresolved, or require further escalation, please contact our DPO.

The DPO's contact details are set out below:

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 (option 1, then option 1 again)

Security and Data Related Policies

We must keep personal data secure against loss or misuse. All staff are required to comply with our information security guidelines and policies. In particular, staff should refer to the following policies that are related to this Data Breach Policy:

- **Security Policy / IT Security Policy:** sets out the School's guidelines and processes on keeping personal data secure against loss and misuse.
- **Data Protection Policy:** sets out the School's obligations under UK GDPR about how personal data is processed.

- **Cyber Security Policy:** sets out the School's obligations and guidelines for cyber security issues.

Data Breach Procedure

What is a Personal Data Breach?

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

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

- Loss or theft of data or equipment on which data is stored (e.g. loss of a laptop or paper file);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (e.g. sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it;
- Alteration of personal data without permission;
- Loss of availability of personal data.

When Does It Need to Be Reported?

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that if unaddressed, the breach is likely to have a significant detrimental effect on individuals.

Examples of significant detrimental effects include:

- Potential or actual discrimination;
- Potential or actual financial loss;
- Potential or actual loss of confidentiality;
- Risk to physical safety or reputation;
- Exposure to identity theft (e.g. release of non-public identifiers such as passport details); and
- Exposure of private aspects of a person's life becoming known to others.

If the breach is likely to result in a **high risk** to the rights and freedoms of individuals, then affected individuals must also be notified directly without undue delay.

Reporting a Data Breach

If you know or suspect a personal data breach has occurred or may occur, you should:

1. Complete a Data Breach Report Form (Appendix 1);
2. Email the completed form urgently to Katie Findlater and the DPO.

Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure. Once reported, you should not take any further action in relation to the breach (specifically, do not notify affected individuals or regulators or investigate further on your own). Katie Findlater will acknowledge receipt and handle the incident in collaboration with the DPO.

Managing and Recording the Breach

On being notified of a suspected personal data breach, the School and DPO will take immediate steps to:

- Establish whether a breach has in fact occurred;
- Contain the data breach and recover, rectify or delete the affected data so far as reasonably practicable;
- Assess and record the breach in the School's Data Breach Register;
- Notify the ICO where required;
- Notify affected data subjects if required;
- Notify other appropriate parties (e.g. insurers, police); and
- Take steps to prevent future breaches.

Containment and Recovery

The designated lead with the support of our DPO will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure. They will identify ways to recover, correct or delete data. Depending on the nature of the breach, the School will notify insurers (Professional Indemnity / Cyber Insurance) to access data breach management experts and notify law enforcement if criminal activity is suspected.

Notifying the ICO

The School will notify the ICO when a personal data breach is likely to result in a risk to the rights and freedoms of individuals. This will be done **without undue delay and where possible, within 72 hours of becoming aware of the breach** (including weekends and school holidays). If the notification is made after 72 hours, written reasons for the delay will be recorded.

Notifying Data Subjects

Where the breach is likely to result in a high risk to the rights and freedoms of data subjects, the School will notify affected individuals directly without undue delay. The notification will include contact details for the DPO and ICO, likely consequences, and measures taken or planned to mitigate potential adverse effects.

Preventing Future Breaches

Following resolution of a breach, the School will review security measures, establish whether human error or systematic issues caused the breach, implement technical or

organisational safeguards, deliver refresher training, update the Data Breach Register, and debrief management and governors.

Reporting Data Protection Concerns

Data security concerns should be reported proactively to Katie Findlater or the DPO to help capture risks early. If you have concerns that your personal data has been involved in a data breach or about your data rights, please refer to the School's Data Protection Policy for details on submitting a data protection complaint.

Appendix 1 – Data Breach Report Form

Time is of the essence with data breaches. Submit this report as soon as you know or suspect there has been a data breach. Do not delay to satisfy yourself whether a breach has definitely happened.

Name & contact details of person notifying:	[Insert name and contact details - or leave blank if anonymous]
Department / Manager:	[Insert department and line manager]
Date of actual or suspected breach:	[Insert date]
Date of discovery of breach:	[Insert date]
Date of this report:	[Insert date]
Summary of the facts:	[Provide detailed summary – including type, sensitivity and amount of data involved]
Cause of actual or suspected breach:	[Provide detailed account of what happened]
Is the breach ongoing?	Yes ☐ No ☐ Not Known ☐
Who is or could be affected?	[Include categories and approximate number of data subjects]
Are you aware of any related breaches?	Yes ☐ No ☐ (If yes, give details)