Data Breach Policy
Full School incl. EYFS

2026-2027

Ibstock Place

CO-EDUCATIONAL DAY SCHOOL

IBSTOCK PLACE SCHOOL

Data Breach Policy

Full School including EYFS

Scope

This policy applies to all pupils (age 3 (EYFS) - 18) and staff at Ibstock Place School (hereinafter 'Ibstock' or 'the School').

Roles and Responsibilities

The Governing Body delegates responsibility to the Head for developing and enacting any required "Good Practice" policies. These policies are non-statutory and do not require ratification by the Governing Body. As such, the Head has delegated accountability and responsibility for the operationalisation of this policy to the Data Manager who ensures the consistent application and implementation of this policy across the School. Staff should follow the expectations set out in this policy, a copy of which is available on the School's SharePoint site.

Introduction

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 to 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 (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data – Previously termed 'Sensitive Personal Data', Special Category Data is similar by definition and 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 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.

Data Subject - Person to whom the personal data relates.

ICO – The ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

Responsibility

The Data Manager has overall responsibility for breach notification within the School and is the designated point of contact for personal data breaches. The Bursar is responsible for ensuring that breach notification processes are adhered to by all staff.

In the absence of the Data Manager, please contact the Head.

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

Please contact the DPO with any questions about the operation of this policy or the UK GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO's contact details are set out below: -

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174

Security and Data Related Policies

Staff can also refer to the following policies that are related to this Data Breach Policy and can be found on the School's SharePoint site.

- Code of Conduct for Staff
- Data Protection Policy
- Data Retention Policy
- E-Safety Policy and Acceptable Use Agreement
- IT and Computing Policy
- Privacy Notices for Staff, Pupils and Parents, Governors and Volunteers, Job Applicants, Visitors and Contractors
- Social Media Policy
- Complaints Policy

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 could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored for example, loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example, 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.

When does it need to be reported?

The School must notify the ICO (Information Commissioner's Office) of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed, the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- 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 (for example, through the release of non-public identifiers such as passport details); and
- The exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

Reporting a Data Breach

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should:

- Email the Data Manager (**Christo Nel: cnel@ibstockplaceschool.co.uk**) with information outlining the breach, providing as much information as possible.

- The Data Manager will follow up with any additional questions and action.

Where appropriate, you should liaise with your Line Manager regarding the breach. Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. You can seek advice from your Line Manager, Data Manager or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must **not** notify any affected individuals or regulators or investigate further. The Data Manager will acknowledge receipt of the data breach email and take appropriate steps to deal with the report in collaboration with the DPO.

Managing and Recording the Breach

On being notified of a suspected personal data breach, the Data Manager will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so, they will take steps to:-

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO where required;
- Notify data subjects affected by the breach if required;
- Notify other appropriate parties to the breach; and
- Take steps to prevent future breaches.

Notifying the ICO

The Data Manager will notify the ICO when a personal data breach has occurred which 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. The 72 hours deadline is applicable regardless of school holidays (i.e., it is not 72 working hours). If the School is unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Manager or a member of the Senior Management Team will notify the affected individuals without undue delay including the name and contact details of the DPO and the ICO, the likely consequences of the data breach and the measures the School has (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the Data Manager will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example, by making a statement on the School website).

Notifying Other Authorities

The School will need to consider whether other parties need to be notified of the breach. For example:

- Insurers
- Parents
- Third parties (for example, when they are also affected by the breach)
- Local authority
- The police (for example, if the breach involved theft of equipment or data)

This list is non-exhaustive.

Assessing the Breach

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover, correct or delete data (for example, notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include:

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e., the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Whether there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What the likely consequences of the personal data breach are on the School; and
- Any other wider consequences that may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we shall:

- Establish what security measures were in place when the breach occurred;

- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- Update the data breach register;
- Debrief governors/management following the investigation.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to the Data Manager or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

Training

The School will ensure that staff are trained and aware on the need to report data breaches to ensure that they know to detect a data breach and the procedures of reporting them. This policy will be shared with staff.

Queries

Queries on this policy should be directed to the Data Manager.

Review and Verification

This policy is reviewed annually, or as required, by the Data Manager. On-going monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.