

Data Breach Policy

September 2026

Version 2

Review Date: September 2028

Version History Log

Date	Version	Description of Change	Changes made by
July 2024 Nov 2024	1	Original Policy created by Judicium Consulting Ltd and adapted for Park Hill Infant School. Reviewed by Judicium Education. Approved at Full Governing Board Meeting 11/11/24.	Stephanie Croucher Amaanat Khaira at Judicium Education.
September 2026	2	Policy updated and reformatted using new template provided by Judicium Consulting Ltd including signposting to data protection complaints procedure in UK GDPR and Data Protection Policy. Due to be ratified at Full Governing Board meeting on Monday 16th November 2026.	Stephanie Croucher

Contents

Data Breach Policy Introduction 2

Definitions 2

Responsibility 3

Security and Data Related Policies 4

Data Breach Procedure 4

- What is a personal data breach? 4
- When does it need to be reported? 4

Reporting a Data Breach 5

- Managing and Recording the Breach 5
- Assessing the Breach 5
- Containment and Recovery 6
- Notifying the ICO 6
- The potential harm to the rights and freedoms of data subjects 6
- The volume of personal data 7
- The sensitivity of data 7
- Notifying Data Subjects 7
- Notifying the Police 8

Preventing Future Breaches 8

Reporting Data Protection Concerns 8

Staff Awareness and Training 9

Monitoring 9

Appendix 1 – Data Breach Report Form 10

DRAFT

Document Owner and Approval

Park Hill Infant School is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the school's policy review schedule.

A current version of this document is available to all members of staff in the schools' shared drive (Teacher Shared) and in a physical copy is kept in the main school office.

Data Breach Policy 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 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.
Data Protection Officer (DPO)	The person we appoint from time to time to lead the development and implementation of our data protection and compliance with the UK GDPR and other applicable.

Responsibility

Stephanie Croucher (Data Compliance Officer) 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 the absence of Stephanie Croucher, please contact Dawn Crosby Per (School Business Manager.)

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: 5th Floor, 98 Theobalds Road, London, WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 opt 1, then opt 1

DRAFT

Security and Data Related Policies

Staff should refer to the following policies that are related to this Data Breach Policy: -

- *LGFL Acceptable Use Policy* which is signed by all staff annually and at the commencement of their employment;
- *UK GDPR and Data Protection Policy* which sets out:
    - the school's obligations under UK GDPR about how the school processes personal data;
    - the school's guidelines and processes on keeping personal data secure against loss and misuse.
- *Cyber Security Policy, Cyber Risk Report and Cyber Response Plan* which sets out the School's obligations and guidelines for cyber security issues.
- *Online Safety Policy*
- *Data in Transit Policy* which sets out the practice for staff to maintain good security when using, taking or sending sensitive or confidential school data outside of its normally secure location.

These policies are also designed to protect personal data and can be found in the schools' shared drive (Teacher Shared) and in a physical copy is kept in the main school office.

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;
- 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 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;

DRAFT

- 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 notify Stephanie Croucher, Data Compliance Officer. A Data Breach Form is attached in Appendix 1.

Where appropriate, you should liaise with your line manager about completion of the data report form. 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. They can seek advice from their line manager, Stephanie Croucher (DCO) or the DPO – Judicium Consulting Ltd.

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. Stephanie Croucher will acknowledge receipt of the data breach 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, Stephanie Croucher 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.

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).

DRAFT

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;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation, two factor authentication);
- What has happened to the data, e.g., if data has been stolen, could it be used for harmful purposes;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

Containment and Recovery

Stephanie Croucher, with the support of our DPO, will identify how the breach occurred and take immediate steps to stop of minimise further loss, destruction or unauthorised disclosure of personal data.

Stephanie Croucher, with the support of our DPO and IT service OpenAIR Ltd, will identify ways to recover, correct or delete data. This may include contacting the police, e.g., where the breach involves stolen hardware or data.

Depending on the nature of the breach, Stephanie Croucher/ Dawn Per, with the support of our DPO, will notify the Risk Protection Arrangement (RPA) so that the insurer can provide access to data breach management experts.

Notifying the ICO

Stephanie Croucher, with the support of our DPO, 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 are 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.

If the school are unsure whether to report, the presumption should be to report. The school will take into account of the factors set out below:

The potential harm to the rights and freedoms of data subjects

This is the overriding consideration in deciding whether a breach of data security should be reported to the ICO. Detriments include emotional distress as well as both physical and financial damage. It can include:

- Exposure to identify theft through the release of non-public identifiers, e.g. passport number;
- Information about the private aspects of a persons life becoming known to others, e.g. financial circumstances;

The personal data breach must be reported unless it is unlikely to result in a risk to data subjects' rights and freedoms.

The volume of personal data

There should be a presumption to report to the ICO where:

- A large volume of personal data is concerned; and
- There is a real risk to individuals suffering some harm.

It will, however, be appropriate to report much lower volumes in some circumstances where the risk is particularly high, e.g. because of the circumstances if the loss or the extent of information about each individual.

The sensitivity of data

There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial detriment, including substantial distress.

This is most likely to be the case where the breach involves special category personal data. If the information is particularly sensitive, even a single record could trigger a report. The ICO provides two examples:

- theft of a manual paper-based filing system (or unencrypted digital media) holding the personal data and financial records of 50 named individuals would be reportable;
- breach of a similar system holding the trade union subscription records of the same number of individuals (where there are no special circumstances surrounding the loss) would not be reportable.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, Stephanie Croucher 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 have (or intended) to take to address the breach, including where appropriate, recommendations for mitigating potential adverse effects.

When determining whether it is necessary to notify individuals directly of the breach, Stephanie Croucher 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).

DRAFT

Notifying the Police

The School will already have considered whether to contact the police for the purpose of containment and recovery. Regardless of this, if it subsequently transpires that the breach arose from a criminal act, the school will notify the police and/or relevant law enforcement authorities.

Notifying Other Authorities

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

- The Information Commissioner s Office (ICO);
- Affected data subjects;
- 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).

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 will:

- 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;
- To update the data breach register;
- To 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 would encourage you to report any concerns (even if they do not meet the criteria of a data breach) that you may have to Stephanie Croucher (DCO) 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.

If you have concerns that your personal data has been involved in a data breach, or you have concerns about a suspected breach of any of your data rights, please refer to the School's UK GDPR and Data Protection Policy for details of how to submit a data protection complaint.

DRAFT

Staff Awareness and Training

Key to the success of our systems is staff awareness and understanding. We provide annual GDPR and Data Protection refresher training to staff via Jedu.co.uk, and we also provide GDPR and Data Protection training:

- At induction;
- When there is any change to the law, regulation or our policy;
- When significant new threats are identified; and
- In the event of an incident affecting our school.

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.

Monitoring

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the school.

This policy is reviewed every two years by the Senior Leadership Team. At every review, it will be approved by the Full Governing Board.

The next scheduled review date for this policy is September 2028.

Signed:_____

Print Name:_____

Date:_____

DRAFT

Appendix 1 – Data Breach Report Form

If you know or suspect a personal data breach has occurred, please:

- Complete this form; and
- Email or deliver it to Stephanie Croucher (via enquiries@parkhill-inf.croydon.sch.uk) and the DPO, ensuring that you mark your email as urgent, with the subject 'Data Breach'.

Time is of the essence with data breaches. You must submit this report as soon as know or suspect there has been a data breach. Do not delay to satisfy yourself whether a data breach has definitely happened and do not contact any individuals who may be affected by the data breach. Stephanie Croucher, along with the DPO, will investigate the potential breach and take necessary actions.

Name and contact details of person notifying the actual or suspected breach	*[Insert name and contact details]* *If you wish to submit an anonymous report, leave this section blank*
Department/manager	*[Insert department from which the report emanated and the relevant manager]*
Date of actual or suspected breach	*[Insert date]*
Date of discovery of actual or suspected breach	*[Insert date]*
Date of this report	*[Insert date]*
Summary of the facts	[*Provide as much information as possible – including the amount, sensitivity and type of data involved*]
Cause of the actual or suspected breach	*[Provide a detailed account of what happened]*
Is the actual or suspected breach ongoing?	Yes ☐ No ☐ Not known ☐
Who is or could be affected by the actual or suspected breach?	*[Include details of categories and approximate number of data subjects concerned]*
Are you aware of any related or other data breaches?	Yes ☐ No ☐ [*If yes, provide more details*]

DRAFT