St. Paul's C of E Primary School

Data Breach Policy

Approved by the Resources Committee: Autumn 2026

Review Date: Autumn 2027

Contents

1. Introduction 3
2. Purpose 3
3. Responsibilities 3
4. Personal data breaches 4
5. Management of data breaches 4
    5.1 Containment and recovery 5
    5.2 Assessment of ongoing risk from breaches 6
    5.3 Notifications 6
    5.4 Evaluation and response 8
6. Staff Notification and Training 9
7. Monitoring 9
8. Complaints 9
Appendix A - Personal Data Breach/Incident Reporting Form 11
Appendix B - Template Data Subject Notification Letter 19
Document Control 21

1. Introduction

St. Paul's C of E Primary School is committed to ensuring that all personal data it processes is handled securely and in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

A personal data breach is defined under Article 4(12) UK GDPR as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data that is transmitted, stored, or otherwise processed. Personal data breaches can result from human error, system failures, loss or theft of information, cyber incidents, or unauthorised access to personal information.

The school is committed to ensuring that all actual or suspected personal data breaches are identified, assessed, recorded, and responded to promptly and effectively. Where required, breaches will be reported to the Information Commissioner's Office (ICO) and, where there is a high risk to individuals' rights and freedoms, to the affected individuals without undue delay.

This policy sets out the school's approach to managing personal data breaches, minimising risks to individuals, and ensuring compliance with legal and regulatory requirements.

2. Purpose

The purpose of this policy is to ensure that the school reacts appropriately to mitigate the risks associated with actual or suspected security incidents relating to information systems and data. The school recognises that there are risks associated with users accessing and handling information to conduct official School business.

This policy applies to all staff employed by our school, Governors and to external organisations or individuals working on our behalf.

The personal information that the school holds must be handled and dealt with securely, regardless of format.

3. Responsibilities

The **Headteacher** 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.

The **Governing board** has responsibility for the oversight of the school's compliance with GDPR.

The Headteacher/School Business Manager is responsible for completing the data breach form and reporting any data breaches to the DPO via igschoolsupport@stockport.gov.uk

The **Data Protection Officer (DPO)** has overall responsibility for monitoring compliance with this policy, overseeing the breach management process and providing risk-based advice to the organisation. The DPO will be the main contact with the ICO.

Line Managers are responsible for ensuring that all staff are aware of their responsibilities to report any breaches of personal data and investigate any incidents.

All staff are responsible for immediately reporting any incident or breach affecting personal data held by the school to the Headteacher or School Business Manager.

4. Personal data breaches

A personal data breach occurs where there is an actual or potential loss of personal information or an unauthorised disclosure of personal data, where the incident could affect an individual's privacy, lead to identity fraud, or have some other significant impact on individuals or the school.

These incidents could occur by a range of means including the information being lost, stolen, accessed, disclosed, or altered without appropriate authority.

The ICO states that a personal data breach/incident can happen for a number of reasons. The most common types of data breaches include:

- Personal data being disclosed to the incorrect recipient via email, post or verbally.
- Cyber incidents – such as hacking or disruption.
- Lack of appropriate checks before disclosure e.g., not redacting third party data.
- Personal data accessed inappropriately or maliciously.
- Personal data disclosed unlawfully or without consent.
- Loss or theft of paperwork or devices holding personal data.

Where a breach involves a contracted processor or supplier, the processor must notify the school without undue delay in accordance with contractual obligations and data processing agreements.

5. Management of data breaches

When an incident occurs, there are four important elements to the incident management plan:

- Containment and recovery
- Assessment of ongoing risk
- Notification
- Evaluation and response.

The GDPR mandates a duty on all organisations in the UK to report certain types of data breaches to the ICO. In some cases, organisations also must notify certain types of data breaches to the individuals affected.

A notifiable breach must be reported to the ICO within 72 hours of the organisation becoming aware of it. It is, therefore, important that staff recognise when an incident has occurred and be able to report it appropriately, so that immediate action can be taken to contain it.

All data breaches must be reported to the Information Governance Team at Stockport Council within 24 hours.

5.1 Containment and recovery

The person discovering a personal data breach should report it immediately as follows:

- to their line manager and the Headteacher or School Business Manager
- to the Information Governance Team, via igschoolsupport@stockport.gov.uk, who will log the incident on the data breach register and advise on the next steps/any immediate action required to contain the incident;
- to any other departments who may need to be involved e.g. HR, ICT.

Near misses should also be reported where a personal data breach was narrowly avoided, enabling lessons to be learned and controls strengthened.

Where a breach involves safeguarding records, child protection information, looked after children, SEND information, or other high-risk pupil information, the incident should be escalated immediately to the Headteacher and DPO.

Breach investigation

At this point an Investigating Officer (usually a Manager) must start a full investigation without delay. The Personal Data Breach Form should be completed and sent to the Information Governance Team within 24 hours.

The Investigating Officer should ensure that they obtain all relevant facts regarding the incident, take possession of any documentation, and record any key facts/decisions from this point forward. As a minimum this should include:

- Date and time of the incident.
- Who was involved.

- Exactly what information has been disclosed.
- How the breach occurred.
- Whether the data has been recovered.
- Whether the individual/(s) whose data was involved in the incident (data subject) are aware of the breach.
- What immediate corrective action has been taken.
- What further actions have been planned.

5.2 Assessment of ongoing risk from breaches

The Investigating Officer must accurately define any risk to the school or individual/s as a result of the breach. This will need to be assessed to allow the school to control and mitigate the risk. The risks associated will be dependent on:

- The type of data involved.
- How sensitive the information is.
- Whether there were any protections in place, e.g., encryption
- What has happened to the data, if known.
- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.
- What harm can come to those individuals whose data has been lost.
- Whether there are any wider consequences to the loss of the data.

5.3 Notifications

Sometimes the school may have to report the breach to the following:

- The Information Commissioner's Office or/and
- the individuals themselves.

Depending on the incident there may be other legal, contractual or sector-specific requirements to notify various parties. The school's Governing Board will be informed about significant personal data breaches and trends in data protection incidents where appropriate.

ICO

The GDPR introduced a duty on all organisations in the UK to report certain types of data breaches to the ICO. If the breach is likely to cause a risk to individual's rights and freedoms it must be reported within 72 hours of the school becoming aware of it. Any ICO notifications will be determined by the Data Protection Officer alongside the school, or in the DPO's absence, the most senior member of the Information Governance team at Stockport Council.

Where the ICO is to be notified, the ICO breach reporting form will be completed by a member of the Information Governance Team, alongside the Headteacher.

The notification to the ICO should include all information known at the time the incident is notified. Further details can be added to the notification as they become known and as the internal process develops.

The ICO will respond to the breach notification and may conduct further investigations. The findings of the ICO investigation may require further changes to policies or procedures or impose sanctions. Any interactions with the ICO regarding breaches should be brought to the attention of the IG team and the investigating officer.

Individuals

Where a personal data breach/incident is likely to result in a high risk to the rights and freedoms of individuals, a data controller must notify those concerned directly, without undue delay. An immediate assessment must be made as to whether the data subject should be notified. This decision should be made following consultation between the DPO and the school.

Notification will include a description of how and when the breach occurred, and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the DPO for further information or to ask questions on what has occurred.

As a rule, it is recommended that the data subject is informed unless you can clearly justify why it is not in the data subject's interest to do so.

Any communication to an affected data subject should contain:

- the name and contact details of the school's DPO;
- describe the likely consequences of the personal data breach;
- describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

A template letter is provided at Appendix B.

Data Subjects will not need to be notified in the following circumstances:

- Where the school has implemented appropriate technical and organisational protection measures and that those measures were applied to the personal data affected by the personal data breach i.e., data was encrypted.
- Where the school has taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to occur.
- Where notification would require disproportionate effort. In such circumstances there would still be an expectation for there to be a public communication or similar measure to notify data subjects

If the Investigating Officer is concerned that an employee may be involved in fraudulent activity, the Headteacher should be contacted for advice.

A record will be kept of any personal data breach, regardless of whether notification to the ICO was required.

Third Parties

The school might consider notifying third parties such as the police, insurers, banks or credit card companies, and trade unions. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

5.4 Evaluation and response

Upon receipt of the completed Data Breach/Incident Reporting Form, the Information Governance Team will assess the incident and the investigation to date and advise on and co-ordinate any further actions required.

The role of the IG Team is to:

- review the circumstances of the incident and assess the actions taken to date.
- consider whether any additional measures are required to prevent a recurrence of the incident or similar breaches.
- identify any organisational, procedural, or compliance issues arising from the breach.
- agree an action plan for implementation and monitoring.

The IG Team will also consider whether the risk of the breach had been identified previously and whether the incident could reasonably have been prevented. This review will include:

- the likelihood of a similar incident occurring again.
- whether the incident occurred despite existing controls and safeguards being in place.
- whether existing controls and mitigation measures were adequate and effective
- if staff had received appropriate training and communication in relation to information governance;
- whether current policies, procedures, and working practices remain suitable or require amendment or improvement.

All Data Protection incidents will be reviewed in accordance with NHS England's; "Guide to the Notification of Data Security and Protection Incidents"

		Likelihood harm has occurred				
		1. None	2. Unlikely	3. Likely	4. Highly Likely	5. Extreme
Impact	1. No adverse effect	1	2	3	4	5
	2. Minor	2	4	6	8	10
	3. Adverse	3	6	9	12	15
	4. Serious	4	8	12	16	20
	5. Catastrophic	5	10	15	20	25

Key	
Low risk	
Medium Risk	
High Risk	ICO
Extreme Risk	ICO

Where an incident is assessed as High or Extreme Risk, the school and DPO will undertake a detailed investigation. Depending on the nature and severity of the incident, the DPO may require a dedicated investigation panel to be established to oversee the response, identify corrective actions, and monitor measures to reduce the risk of further harm or recurrence.

Consideration should be given to whether the incident resulted from deliberate misuse of personal data or a failure to follow policies and procedures. Where appropriate, the matter may be referred to the Headteacher and HR for consideration under the school's disciplinary procedures. Corrective actions may include additional training, supervision, or formal management action

6. Staff Notification and Training

Where changes are made to policies, procedures, systems, or working practices as a result of a personal data breach, all relevant staff will be informed and provided with updated guidance.:

Following a breach, the school will consider whether additional information governance training or awareness activities are required. Staff may be required to complete refresher or targeted training to help prevent similar incidents and support compliance with data protection requirements.

7. Monitoring

The IG Team will monitor the implementation and progress of action plans for all incidents on a regular basis to ensure that follow-up action is taken to avoid repeat incidents occurring.

8. Complaints

Individuals who have concerns about how the school has handled a personal data breach can contact the school in the first instance. Complaints will be investigated

and responded to in accordance with the school's complaints procedures. Individuals may also contact the school's Data Protection Officer via igschoolsupport@stockport.gov.uk or raise concerns with the Information Commissioner's Office (ICO).

Appendix A - Personal Data Breach/Incident Reporting Form

Stage 1 - To be completed by Investigating Officer

Please refer to the Personal Data Breach Policy while completing this form

Personal Data Breach/Incident Reporting Form	
School Name	
Date of incident	
Investigating Officer	
Head Teacher	
Type of breach	Choose an item. Other:

Describe the breach

You must not record the personal details of those involved in the breach or those affected by the breach on this form. Please use 'pupil' / 'teacher'/ 'parent' etc. instead of the name of the subject.

Description of breach • **What has happened (no acronyms)** • **Who was involved (do not use individual's names)**
How did you find out about the breach?
When did you discover the breach?

Date: Time:
When did the breach happen?
Date: Time:

Categories of personal data breached					
☐	Basic personal identifiers e.g. Name, contact details	☐	Criminal convictions/ offences	☐	Data revealing racial or ethnic origin
☐	Finance e.g. Credit card, bank details	☐	Religious or philosophical beliefs	☐	Political opinion
☐	Location data	☐	Safeguarding/child protection information	☐	Sex life data
☐	Identification data e.g. username	☐	Gender reassignment data	☐	Health data
☐	Image (i.e. photograph, film)	☐	Genetic or biometric data	☐	Not Known
☐	Other – specify				

Number of people affected	**Estimated number of records affected**

Categories of people affected			
☐	Pupils (under 13)	☐	School Staff
☐	Students (13-18)	☐	Governors
☐	Parents/Guardians	☐	Not known
☐	Other – please specify:		

Potential consequences of the breach • **What impact could occur to individual(s), because of the breach?** • **Has any actual harm occurred to the individual(s)?**

Does any other service area need to be informed?			
☐	IT (ie loss of equipment)	☐	HR (ie staff not following procedure)
☐	Caldicott Guardian (loss of LAC social care data)	☐	Communications (reputational damage)
☐	Legal	☐	Safeguarding
☐	Other:		

Risk Analysis Grading

(*Please refer to Personal Data Breach Policy for further guidance*)

Risk Analysis– (*Please answer the below questions to help determine potential risk to the data subject(s))*		
1.	Number of people's data breached	Choose an item.
2.	Who was the data disclosed to?	Choose an item. Choose an item.
3.	Types of data	Choose an item. Choose an item. Choose an item.
4.	Likelihood of data subjects suffering significant consequences as a result of incident?	Choose an item.
5.	Risk Factors	Choose an item. Choose an item. Choose an item. Choose an item.

Reflections

Describe the measures you have in place to prevent this type of breach occurring in the first place e.g. staff training, processes/procedures, system controls etc.

Has this type of incident happened before? If so, provide a brief summary of when, who was involved, outcome.	
What actions have been taken now to minimise risk of reoccurrence?	
Do the data subjects know or have you told them about the breach?	
☐ Yes	☐ No
Further action planned – Provide details of all further actions yet to take place	

Please e-mail the completed form to: igschoolsupport@stockport.gov.uk

If you require further advice in relation to this incident, please contact the Information Governance Team

Stage 2 – Completed by the Information Governance Team

Type of incident (ICO)
Choose an item.

Type of incident (Internal)
Choose an item.

Number of people affected	Estimated number of records affected

Investigation chronology:		
Date	**Description**	**Further Action**

Further questions	
Were there measures in place to prevent an incident of this nature occurring?	Choose an item.
Are there any policies and procedures considered relevant to this incident?	Choose an item.
Does this incident involve any financial/special category or safeguarding data?	Choose an item.
Are the affected individuals aware of the incident?	Choose an item.
Have any affected individuals complained to the organisation about the incident?	Choose an item.
Has the data now been recovered?	Choose an item.
Had the relevant staff members involved in this incident received training?	Choose an item.

Risk Analysis Grading

Risk analysis review – likelihood of harm

Likelihood harm has occurred

Number	Likelihood harm has occurred	Description
1.	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trial or forensic evidence.
2.	Not likely or any incident involving vulnerable groups even if no adverse effect occurred.	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3.	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4.	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5.	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

Likelihood score *(Using the table above please select your chosen score and explain why)*
Choose an item. Comment:

Risk analysis review - potential impact on individuals

Potential impact on individuals

Number	Impact on individuals	Description
1.	No impact	There is absolute certainty that no adverse effect can arise from the breach – no impact
2.	Minor	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred. A minor adverse effect must be selected where there is no absolute certainty.
3.	Adverse - Potentially some adverse effect	An adverse effect may be release of confidential information to into the public domain leading to embarrassment or it prevents someone from doing their job.
4.	Serious - Potentially pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. (i.e. loss of bank details leading to loss of funds/loss of employment.
5.	Catastrophic - Death/catastrophic event	A person dies or suffers a catastrophic occurrence

Impact score
Choose an item. Comment:

		Likelihood harm has occurred				
		1. None	2. Unlikely	3. Likely	4. Highly Likely	5. Extreme
Impact	1. No adverse effect	1	2	3	4	5
	2. Minor	2	4	6	8	10
	3. Adverse	3	6	9	12	15
	4. Serious	4	8	12	16	20
	5. Catastrophic	5	10	15	20	25

Key	
Low risk	
Medium Risk	
High Risk	ICO
Extreme Risk	ICO

Scale of risk	
Score:	**Risk Level:** Choose an item.
Comment:	

Scale of risk following mitigations	
Score:	**Risk Level:** Choose an item.
Comment:	

Recommended Actions				
Date	**Action**	**Responsible**	**Due Date**	**Complete Date**

Next Steps	
Does the risk score require the incident to be referred to the DPO?	Choose an item.
Is there any other reason why this incident should be referred to the DPO?	Choose an item.
IG Officer	

Stage 3 – Data Protection Officer Review

Data Protection Officer Review			
Is this incident to be referred to the ICO?	Choose an item.	**Date referred**	
DPO sign off		**Date**	

Appendix B - Template Data Subject Notification Letter

Important information about your personal data

I am writing to inform you of a personal data breach involving information held by **[School Name]**.

We recently became aware of an incident which resulted in the unauthorised disclosure, loss, alteration, or access to personal information relating to you.

What happened?

[Provide a clear explanation of the incident, including:]

- What happened and when it occurred.
- How the school became aware of the incident.
- What personal information was involved.
- Whether any special category information was affected (for example, health, safeguarding, SEND, or other sensitive information).
- Whether the information was disclosed to an unauthorised person or otherwise compromised.

What we have done

We take the security and confidentiality of personal information very seriously. As soon as we became aware of this incident, we took steps to contain the breach and minimise any potential impact.

Actions taken include:

- [Detail immediate containment actions.]
- [Explain any recovery actions taken.]
- [Explain how the incident occurred, if known.]
- [Outline any changes to processes, procedures, systems, or training to prevent a similar incident happening again.]

What this means for you

At present, [provide an assessment of any known risks to the individual].

To help protect your information, we recommend that you:

- [Insert any relevant advice for the individual.]
- [Monitor accounts or correspondence if applicable.]

- [Change passwords or security information if relevant.]

We have also implemented the following additional measures to protect your information:

- [Detail any specific safeguards offered.]
- [Detail any account security measures, password resets, or enhanced monitoring arrangements.]

If you would like to discuss any further measures available to help protect your information, please contact us using the details below.

Further Information

If you have any questions about this incident, please contact:

[Name and Job Title]
Telephone: [Insert number]
Email: [Insert email address]

You may also contact our Data Protection Officer:

Information Governance Team
Email: igschoolsupport@stockport.gov.uk

Our Apology

Please accept our sincere apologies for this incident and for any concern or inconvenience it may cause. We understand the importance of keeping personal information secure and regret that this incident occurred.

Yours sincerely,

[Name]
[Job Title]
[School Name]

Document Control

Title	Personal Data Breach Policy
Document Owner	Information Governance – Stockport Metropolitan Borough Council
Document Status	For School Approval
Links with other policies, procedures, or guidance	Data Protection Policy
Target Audience	School workforce, School governors
Distribution	Website, hard copy
File Classification	Public
Current Version	7.0

Revision and Approval

Reviewed by	SMBC IG Team
Issue Date	01/09/2026
Approved by (school)	TBC
Approval date	TBC
Next review date	01/09/2028
Any changes made	s1 - changes to Introduction s5.1 - extra section around safeguarding records s8 - complaints section added Appendix A - minor changes to form Appendix B - Template Letter reviewed and refreshed

Change History

Version	Author	Issue Date	Review date	Changes made?
V1	IG Team	15.06.2018	01.09.2019	No Changes
V2	IG Team	01.09.2019	01.09.2020	No Changes
V3	IG Team	23.09.2020	01.09.2021	Annual review
V4	IG Team	10.11.2021	01.09.2022	Update to contacts and Appendix 3
V5	IG Team	28.10.2022	01.09.2024	Terms changed from 'SIGI' to 'data breach'. Minor formatting
V6	IG Team	23.08.2024	01.09.2026	Full review