Information Security Incident Management Policy

St. Paul’s Peel CE Primary School

This policy applies to all employees and governors including temporary, contract staff and anyone who undertakes work on behalf of St Paul’s Peel CE Primary School regardless of their location

Version: 2

Document control

Version control/History

Name	Description	Date
Andrew van Damms	V1.0 Data Incident and Breach policy template for schools	31/08/18
Debbie McCarron	V2 updated references to UK GDPR	March 2021

Approvals

Name	Position	Date

1. Introduction

All schools have a duty under the sixth principle of Article 5 of the UK General Data Protection Regulation (UK GDPR) to take appropriate technical and organisational measures to protect the personal data from unauthorised or unlawful processing, accidental loss, misuse, destruction, and damage. St Paul's Peel CE Primary School takes these responsibilities very seriously and has implemented robust physical and technical security measures.

The school recognises that information security incidents can still occur due to human error, wrongdoing, or other unforeseen circumstances. As well as having preventative and protective measures in place, it is critical that the school is properly prepared to react and take rapid remedial action if something goes wrong. This is reinforced by the requirement to report qualifying data breaches to the regulatory body – the Information Commissioner's Office – within 72 hours.

This policy sets out how the school will deal with information security incidents. It describes the actions that members of staff need to take and outlines the roles and responsibilities of school leadership in deciding whether an incident which amounts to a personal data breach should be reported to the Information Commissioner's Office and any other actions which may need to be taken in order to protect individuals from any potential harmful consequences which may result from that breach. The policy also sets out the advisory role of the Data Protection Officer.

All members of staff are required to familiarise themselves with this policy and comply with the provisions contained in it. This policy is to be read in conjunction with the Data Protection Policy and Records Management policy along with other relevant guidance.

2. Roles and responsibilities

The Headteacher has overall responsibility within the School for managing Information security and the school's overall response to information security incidents. In the absence of the Headteacher, the Deputy Headteacher will assume this responsibility. In practice the School Business Manager will often play a key role in coordinating the school's response to incidents. The Data Protection Officer (and the council's Information Governance Team) are available in an advisory capacity through the SLA service to assist where the school is uncertain what actions may be required in response to an incident.

The Data Protection Officer (DPO) is responsible for overseeing this and other Data Protection policies. The DPO's contact details are below:

Information Governance Team
Salford City Council
Civic Centre
Chorley Road
Swinton
M27 5AW

Email: infogovernance@salford.gov.uk
Tel: 0161 603 6804

3. Information security incidents

Information Security is defined as the preservation of:

- **Confidentiality**: information is accessed only by those authorised to do so
- **Integrity**: safeguarding the accuracy and completeness of information
- **Availability**: authorised users have access to the information they need, as and when they need it.

Information security incidents can take a variety of forms where the confidentiality, integrity or availability of data (paper or electronic) is affected. They do not always involve personal data breaches. A personal data breach is a type of information security incident.

Examples of information security incidents:

- Loss or theft of data
- Unauthorised or unintentional access to data
- Unauthorised alteration of data
- Loss of network service or business system impacting on availability
- Sharing passwords
- Insecure disposal of data

Specific examples of the types of incident which may occur within a school environment include:

- Personal data about a pupil sent to the wrong address (via email or post)
- Disclosure of private email addresses when contacting many parents
- Inappropriate disclosure of pupil's information to absent parent
- Loss of unencrypted USB stick including pupil data
- Loss or theft of mobile device; laptop, smartphone etc
- Weak passwords used to access child information through online parent portal

Information security is a serious matter, as breaches can have negative, far-reaching results including:

- Disruption to, or loss of services
- Loss of revenue by fraud or theft
- Monetary fines – e.g. the Information Commissioner's Office can impose hefty fines
- Reputational damage
- Upset, embarrassment and/or financial loss to individuals if their confidential information was to be lost or accessed by unauthorised persons

4. Incident Management Procedure

Upon discovering an information security incident, immediate action is necessary. If the incident involves personal data, the focus should be on **containment** and **recovery.**

The priority is to act quickly in order to seek to contain the incident, recover the personal data affected and regain control of the situation. Such actions are intended to reduce risk and the possibility of harmful consequences to the individual(s) affected.

In all cases, staff should:

- Depending on the nature of the incident, take any immediate steps to recover/contain the personal data affected. If unclear of what to do, speak in the first instance to the School Business Manager, Headteacher or Deputy Headteacher depending on availability
- If the School Business Manager/Headteacher/Deputy Headteacher are uncertain what to do and urgent advice is required, they will contact the DPO/council's Information Governance team for assistance
- Once all immediate available actions have been taken to contain the incident, the Headteacher/Deputy Headteacher and School Business Manager in collaboration with the DPO, will assess the implications and impacts of the incident and decide whether it is one that needs to be reported to the ICO and whether the individual(s) affected need to be notified (if they are not already aware). They will also review the incident to determine whether any other actions need to be taken e.g. any changes or improvements need to be made to processes, working practices etc in order to prevent or reduce the possibility of such incidents occurring in future.

In practice, immediate steps/actions in the aftermath of an incident may be agreed through urgent discussions. It is very important, however, that full details and actions are documented, initially via the incident form to be followed by a more detailed incident report once the full picture has emerged. The school will also maintain a log of all incidents and outcomes.

5. Reporting to the ICO and notifying individuals

Not all personal data breaches need to be reported to the ICO. In accordance with the UK GDPR, qualifying personal data breaches must be reported to the ICO **within 72 hours**. The DPO will decide whether or not to report the incident.

A qualifying personal data breach is defined in the UK GDPR as one which may result in:

"physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

Essentially breaches which could potentially cause some form of harm, detriment or damage to the individual(s) affected. If there is negligible or no impact, the incident will not warrant notification to the ICO. Any incident that is not reported to the ICO will still be recorded on school's data incident log and any lessons to be learned will be acted on e.g. by implementing process improvements, strengthening procedures, providing refresher training/briefings that may be required.

Individual(s) who are affected by a personal data breach do not need to be informed in all cases. They should be notified in cases where the breach is likely to cause some form of harm, detriment or damage. There needs to be a clear purpose and reason for taking this step and individuals - if there is negligible or no impact then there will be no need to inform the individual(s). The DPO will help to decide whether or not to inform those affected.

6. Near misses

Near misses are incidents which, after investigation, do not actually amount to a personal data breach. Although near misses may not amount to personal data breaches, they should still be recorded in the school's data incident log. In addition, the school recognises that near misses can expose potential areas of weakness and will ensure appropriate actions are taken to strengthen procedures or improve practices.

7. Report to Chair of Governors

The school recognises it is crucial that information security has a high profile and receives regular scrutiny through the school's governance structures.

8. Monitoring Arrangements

The Head is responsible for monitoring compliance with this policy. Failure to adhere to this policy may result in breaches of legislation and affect the school's ability to deliver its services and to demonstrate that it is open and accountable.

The policy template will be reviewed annually and updated if necessary as part of the IG SLA.

The school will ensure that all staff are aware of and have read this policy.

Appendix 1.

Data incident reporting form	
Date and time of incident (or when first became aware of incident)	
Nature of incident (e.g. theft/loss of equipment containing personal data, disclosure of personal data to a third party)	
Full description of incident	
Was any controlled access data (e.g. personal data) lost, stolen, or disclosed in the incident	
Provide a description al all types of personal data involved e.g. name address, health information. **Do not include any information which would identify the individual(s) concerned**	
Number of individuals affected	
Details of any initial steps taken to contain the incident or reduce any ongoing risks.	
Has the data been retrieved or deleted? If yes, please state when and how Is there any evidence that any personal data was further disclosed?	
Who (within school) became aware of the incident?	
How did they become aware of the incident?	
Form completed by	
Position	
Date	