Data Incident and Breach management policy

PRIMROSE HILL
PRIMARY SCHOOL

This policy applies to all employees and governors including temporary, contract staff and anyone who undertakes work on behalf of *Primrose Hill Primary School* regardless of their location

Effective date: September 2018

Document control
Version control/History

Name	Description	Date
Andrew van Damms	V1.0 Data Incident and Breach policy template for schools	31/08/18

Approvals

Name	Position	Date
A Ferns	**Chair of sub-committee**	**September 2020**
A Ferns / D Dobson	**Chair of sub-committee / CoG**	**September 2021**
A Ferns	Chair of sub-committee	September 2022

Decision to review/approve every other year. Next approval date Autumn 2024

1. Introduction

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

The school recognises that data 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 qualifying data breaches are reported to the regulatory body – the Information Commissioner's Office – within 72 hours.

This policy sets out how the school will deal with any data 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. Training and awareness sessions will be provided to all staff.

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. The Data Protection Officer contracted by the school will be immediately contacted in any situation where security may have been breached.
The DPO is responsible for overseeing this and other Data Protection policies.

The school's DPO details:

Data Protection Officer: Craig Stilwell

Company: Judicium Consulting Ltd

Judicium Consulting Ltd
72 Cannon Street
London
EC4N 6AE

Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174

The council's Information Governance Team are also available in an advisory capacity to assist where the school is uncertain what actions may be required in order to address an incident.

SCC's DPO' contact details are below:

Andrew Van Damms
Legal & Governance Division
Service Reform
Salford City Council
Civic Centre
Chorley Road
Swinton
M27 5AW

Email: andrew.vandamms@salford.gov.uk
Tel: 0161 793 3957

3. What is a personal data breach?

Information security incidents can take a variety of forms. They do not always involve personal data – other examples of types of information that can be affected include business sensitive or commercially sensitive information. This policy focuses on incidents which involve personal data. A personal data breach is a type of information security incident where the confidentiality, integrity or availability of personal data (in any form, paper or electronic) has been affected. It will typically result from a process or system failure.

Examples

- Loss or theft of personal data,
- Unauthorised (or unintentional) access to personal data
- Alteration of personal data without permission
- Loss of network service or business system impacting on availability of personal data
- Security breach on the school's network infrastructure, either by accident or malicious intent
- Transmitted insecurely or uploaded inappropriately to a webpage
- Disposed of in an unsecure manner

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 – e.g. about a hearing to investigate complaints about exclusion from school

• Disclosure of private email addresses – e.g. parents email addresses placed in CC field rather than BCC field

• Text message regarding a specific pupil intended for their parents only sent to all parents in error a pupil's

• Inappropriate disclosure of pupil's information to absent parent

• Sending Special Category Personal Data via unprotected email when encrypted email should have been used

• Loss of unencrypted USB stick including pupil data (academic progress)

• Loss or theft of unencrypted laptop or other mobile device e.g. stolen from member of staff's home or car

• Parent passwords to access child information through online parent portal not sufficiently strong resulting in accounts being compromised

3. Priority Actions

Upon discovering a data incident, the immediate priority is **containment** and **recovery.**

Example:

Correspondence being sent to the wrong postal address or an email has been sent to the wrong recipient. It is imperative that steps are taken to attempt to retrieve the data so that the school regains control of the information as quickly as possible and prevent any risk of further dissemination. In the case of email, a member of staff should make attempts to recall the message if this option is available. If this option is unavailable or unsuccessful, the recipient should be contacted and asked to delete the message and to confirm this has been done. In this scenario those actions can be taken immediately by a member of staff without needing to wait for advice and instructions on what to do. In the event that correspondence is sent to the wrong postal address steps will be taken, usually via the School Business Manager/school office staff, to arrange to collect the item of post from the recipient in person.

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 (please see example above). 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
- Ensure that the standard data incident form is completed and sent to the Headteacher, Deputy Headteacher and School Business Manager
  - this will ensure that all relevant details are captured, that there is no single point of failure (e.g. through unavailability) and that any incident is fully investigated and all appropriate actions are taken. The standard data incident form can be found in appendix 1 at the end of this policy.
- Once all immediate available actions have been taken to contain the incident, the Headteacher/Deputy Headteacher and School Business Manager in collaboration will assess the implications and impacts of the incident and decide whether it is one which 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. The School can contact the DPO/council's Information Governance team for advice.

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 spreadsheet of all incidents and outcomes.

4. Reporting to the ICO and notifying individuals

Not all personal data breaches need to be reported to the ICO. In accordance with the GDPR, qualifying personal data breaches must be reported to the ICO **within 72 hours**.

A qualifying personal data breach is defined in the 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 spreadsheet 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).

> Example:
>
> A number of ParentPay accounts are compromised following a malicious attack. As part of this bank account details are stolen exposing parents to the risk of fraud. The parents affected should be informed of the incident as there is clear potential for damage. There is a clear purpose in informing parents as it would enable them to contact their bank, monitor their bank account for any unusual activity and protect themselves from potential fraud.

5. Near misses

Near misses are incidents which, after investigation, do not actually amount to a personal data breach. For example an incident which appeared at first to be a personal data breach, after investigation, did not involve any information from which individuals can be identified. Another scenario could be a disclosure of personal data which had initially been believed to be without authorisation but upon further investigation was a legitimate disclosure of information.

Although near misses may not amount to personal data breaches, they will still be recorded in the school's data incident management spreadsheet. 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.

6. 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. In addition a report will be produced annually and presented to the Chair of Governors providing an outline of any data breaches or near misses which have been recorded along with details of any actions taken.

7. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy. The policy will be reviewed annually and updated if necessary.

The school will ensure that all staff are aware of and have read this policy. This policy will also be shared with the full governing board.

8. Links with Other Policies

This policy is linked to other policies including:

- Data Protection policy
- Records Management and Retention policy
- School records retention schedule

Appendix 1. Data incident reporting form

Summary of Incident	
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	
Personal data	
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	

Impact of incident	
What harm, if any, may result from the incident e.g. in the event financial details are compromised, could individuals affected be exposed to fraud	
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?	
Additional details to assist investigation of incident	
Who (within school) became aware of the incident?	
How did they become aware of the incident?	
Form completed by	
Position	
Date	