Park Road Academy Primary School

Data Breach Policy 2024 - 2026

Contents

1. Introduction and Overview

1.1 What is a Serious Information Governance Incident?

A Serious Information Governance Incident ('SIGI') occurs where there is:

- an actual or potential loss of information or
- an unauthorised disclosure of information,

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. It should be noted that this is not an exhaustive list.

A Serious Information Governance Incident involving personal information is likely to constitute a breach of the General Data Protection Regulation ('GDPR') and the Data Protection Act 2018.

Further guidance on what constitutes a personal breach under GDPR can be found on the ICO website at:

ICO Guidance

Detailed guidance has also been provided by the European Commission Article 29 Working Party and can be accessed at:

Article 29 Working Party Guidance

1.2 What causes a SIGI?

The Information Commissioner's Office (ICO) states that a SIGI/data security breach can happen for a number of reasons:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as fire or flood;
- Hacking attack; or
- 'Blagging' offences where information is obtained by deceiving the organisation that holds it.

Other reasons for a breach occurring could include:

- Poor disposal of confidential waste;
- Unauthorised disclosure of confidential information to a third party (in any format including verbal);
- Finding confidential information/records in a public area; or
- Sharing of computer ID's and passwords.
- Not updating records when we are notified of a change.

1.3 How can a SIGI be managed?

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

1) Containment and recovery;
2) Assessment of on-going risk;
3) Notification;
4) Evaluation and response.

The GDPR has introduced a duty on all organisations in the UK to report certain types of data breach to the Information Commissioner's Office ('the ICO'). In some cases, organisations will also have to report certain types of data breach to the individuals affected.

A notifiable breach has to be reported to the ICO within 72 hours of the School becoming aware of it. It is, therefore, important that staff recognise when an incident has occurred and report it appropriately so that immediate action can be taken to contain it. All incidents must be reported to the Senior Responsible Individual (S Breen) within 24 hours.

2. How to manage an incident – Stage 1

2.1 Containment and recovery

The person discovering a Serious Information Governance Incident should report it immediately to the Senior Responsible Individual (SRI), either in person, by email via SRI@parkroadacademy.co.uk or by telephone on 0161 972 4820. The SRI will log details of the incident and advise on the next steps and/or any immediate action required to contain the incident.

The SRI must start a full investigation without delay. The Serious Information Governance Incident Reporting Form ('Appendix 1') should be completed.

The SRI should ensure that they obtain all the pertinent 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 data subjects involved have been informed;
- What immediate corrective action has been taken; and
- Further actions planned: who is responsible for ensuring they are carried out and when will they be completed.

2.2 Risks from Incident

The SRI must accurately define any risk and this will need to be assessed to maximise the School's ability to control and mitigate the risk. The Severity Table in Appendix 2 gives broad guidelines on assessing the severity of incidents.

The report will need to identify what types of data are involved in the incident. Personal data is any information which identifies living individual and tells you something about them. It does not have to include their name if other information identifies them. This could include:

- Health or Social Care data;
- Financial data (e.g. bank details);
- Personal identification data (e.g. address, N.I. Number); or
- School year group together with initials etc.

The report also needs to consider what impact the incident could have on individuals:

- Is it a 'special category of personal data' as defined Under Article 9 of the General Data Protection Regulation? i.e. data relating to:
    - racial or ethnic origin;
    - political opinions;
    - religious or philosophical beliefs;
    - trade union membership;
    - health;
    - genetic data or biometric data for the purpose of uniquely identifying a natural person
    - sexual life or sexual orientation.

- Is it generally perceived as sensitive data because of what might happen if it is misused e.g. bank account details, information that could cause embarrassment to the individual?

- Are there any protections in place such as encrypted laptop, USB sticks, secure emails etc.?

- How many people are affected by the incident?

- How serious might the effect of the incident be on those people?

    Factors to consider include:

    - physical risk;
    - financial risk;
    - identity fraud risk;
    - damage to personal reputation;
    - negative impact on their privacy;
    - damage to organisational reputation;
    - disclosure of sensitive personal information.

- What is the likelihood of the identified risk occurring? E.g. if IT equipment is stolen, would someone need very specialist equipment and knowledge to access the information?

- Whose data is involved? E.g. Parents, pupils, staff or suppliers?

- What are the possible consequences for the Schools reputation?

- Could there be a risk to public health?

2.3 Notification

As described in Section 1.3 above, the GDPR introduced a duty on all organisations in the UK to report certain types of data breach to the ICO.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly without undue delay. Depending on the incident there may be other legal, contractual or sector-specific requirements to notify various parties.

Notifications may assist in security improvements and implementation, as well as risk mitigation.

An immediate assessment must be made as to whether the data subject (i.e. the individual(s) whose data was involved in the incident) should be notified. This should consider:

- Is the breach likely to result in a high risk to the rights and freedoms of the data subject? Examples of high-risk processing can include:

- Systematic and extensive automated profiling
- Large-scale processing of special categories of data;
- Large-scale, systematic monitoring of a publicly accessible area;
- Other activities that are 'likely to result in a high risk for the rights and freedoms of individuals'

- How notification can help the individual?

- Whether notification would result in undue stress, outweighing the benefit of notifying them?

- Are the individuals who would be notified capable of understanding the notification? For example, does the person have the capacity to understand? If not, you may need to notify a third party with the legal right to make decisions on their behalf (e.g. a Power of Attorney). Consideration will also need to be given as to who needs to be notified when the individual concerned is a child.

- Are the numbers involved so large that notification would involve disproportionate effort? In order to establish if notification would involve disproportionate effort, you would need to take into account the difficulties which would occur in the process of notifying against the potential benefit that the notification might bring to the individual.

- As a general rule, it is recommended that the data subject is advised unless you can clearly justify why it is not the data subject's interest. A template letter is provided at Appendix 3. As a minimum any communication to an affected data subject should contain:

    - the name and contact details of the Schools SRI;
    - 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.

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

- Where the School has implemented appropriate technical and organisational protection measures (in particular those that render the personal data unintelligible to people not authorised to access it) and that those measures were applied to the personal data affected by the personal data breach. An example of this would be that the 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 materialise.

- 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 SRI is concerned that an employee may be involved in fraudulent activity, the School's Senior Leadership Team/Chair of Governors should be contacted for advice.

3. SRI investigation and evaluation – Stage 2

Upon completion of the completed SIGI Reporting Form, the SRI will assess the incident and the investigation to date, and advise on and co-ordinate any further actions required.

The role of the SRI is to:

- review the circumstances of the incident and the action taken so far
- evaluate the circumstances in which the incident took place
- consider whether or not any further action needs to be taken to avoid further breaches or similar incidents occurring
- identify any corporate issues arising from the breach
- agree an action plan, responsible officers and relevant timescales for implementation of follow-up of the incident

The SRI will also review whether or not any risk of the breach occurring had been identified prior to the incident and whether or not it was avoidable. If so:

- did the incident occur despite existing measures being in place?
- were current policies and procedures followed? If not, why not?
- in what way did the current measures prove inadequate?
- had staff received appropriate training and communication in relation to information governance?

- if current procedures and policies were inadequate, how can they be improved e.g. by revision and rewriting, training etc.? If not:
    - how likely is the incident to recur?
    - could changes to current policies and procedures have prevented or lessened the impact of the incident?
    - should current policies and procedures be rewritten?

Consideration also needs to be given to whether or not the incident involved deliberate or reckless behaviour by an employee:

- For a deliberate act, disciplinary measures or prosecution should be considered, taking advice from Legal and HR.
- For reckless behaviour, disciplinary measures and retraining, as appropriate should be considered, taking advice from HR.

The SRI should also consider if the employee concerned in the incident was aware of current policies and procedures.

- If yes, did they comply?
- If not, why not?

Finally, the SRI will conduct a further risk assessment on the incident (Section 2 of the Serious Information Governance Incident Reporting Form in Appendix 1).

4. ICO Notification

ICO Notification will be determined by the Senior Responsible Individual. Where the ICO is to be notified, the ICO breach reporting form will be completed by the SRI.

The notification to the ICO should include as much information pertinent to the incident as is known at the time the incident is notified. Further details can be added to the notification as they become known and as the internal SIGI 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 School breaches should be brought to the attention of the Headteacher.

5. Staff Notification and Training

Where policy or procedure changes are introduced, all relevant staff should be informed of the changes and required to record their acknowledgement of reading and understanding the changes.

There may also be a requirement to repeat, extend or revise training. All involved staff should be required to undertake any new or repeated training resulting from the incident.

6. Monitoring

The SRI 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.

If further information is required relating to this policy please speak to the SRI.

Policy review by Mrs S Breen

Ratified by All Governors April 2024

Serious Information Governance Incident (SIGI) Reporting Form

Stage 1: To be completed by the Senior Responsible Individual

Serious Information Governance Incident Reporting Form	
School name	Park Road Academy Primary School
Date of incident	15th September 2021
Office location	Main Office
Investigating Officer	S Breen
Information Asset Owner	PRAPS
Type of Data - Is it personal data / special category or non-personal data?	Personal data Some special category data
How many individuals affected?	1
Data Lost / Recovered	n/a

Please provide as much detail as possible using the questions as prompts. Do not provide the personal details of those involved in the breach or those affected by the breach. E.g. Use 'service user' and instead of the name of the subject.

Details of incident

Chronology and explanation of how the incident happened? Including:

- Dates and times
- Who was involved and advised
- Explanation of any delay in reporting the incident

On 15/9/21 at 10:49, an email was sent in error to the parents of 11 different families in Reception class. The email was supposed to include a blank health questionnaire for parents to fill in and return regarding their child. However, a previously completed version of the questionnaire by another parent was attached by mistake.

At 11:18 on the same day, the error was discovered and the erroneous email was recalled and the recipients were contacted asking to delete and disregard the email.

The SRI (myself) was also informed and standard procedures were followed in line with our Data Breach Policy. The parents of the pupil involved were notified of the breach via email. The ICO were contacted through their Live Chat system (transcript copy on record) and the ICO's

self-assessment for reporting to ICO was completed. The risk to the pupil was considered unlikely and therefore the ICO were not notified, and internal investigation was completed.
What measures were in place to prevent the incident happening? Including: • Details of staff training • Processes, policies and procedures • Physical and technical controls **Documents containing personal information of pupils are stored securely on our network. The error arose from the naming of documents, and this has since been addressed as part of our internal procedures.**
What are the potential consequences? Including: • Impact on data subject • Organisational impact e.g. on School, service/team **Although the document which was sent in error contained some medical information, the risk to the pupil involved is considered 'unlikely'. The child did not have any medical conditions to list, and a breach of their immunisation record is unlikely to cause harm.** **Minor change made to internal procedures (regarding renaming of incoming files) to eliminate risk of same error reoccurring.**

Corrective action already taken – Provide details of all steps taken to recover and contain the incident
Have the affected individuals been informed (when/how)? If not, advise why not. Yes, informed on same day as breach via email. Copy kept for records.
Has this type of incident happened before? If so, provide a brief summary of when, who was involved, outcome. No**.**
What actions have been taken to minimise risk of reoccurrence? E.g. staff training, changes to processes/procedures, changes to system controls etc. Processes have been updated with regards to renaming of incoming files and their storage.
Any other actions taken? E.g. where the incident involves the loss of IT equipment have IT been informed? See transcript of online chat with ICO See screenshot of ICO self-assessment for informing ICO of breach
Further action planned – Provide details of all further actions yet to take place

Severity Table

NB: This table only gives broad guidelines on the severity of incidents. Each case may differ depending on other variables e.g. the number of people affected, the type of information concerned etc. The severity of each incident should therefore be considered on an individual basis.

Incident Type	**Breach of** (Confidentiality, Integrity, Availability & Accountability)	Severity
Unauthorised access to Network/ Systems/ Applications/Email	Integrity/ Confidentiality/ Availability & Accountability	Moderate to Major depending on the level of information accessed
Sending information		
Information sent to the wrong recipient (internally), disclosing information that is neither confidential not personal	Integrity	Minor
Information sent to various recipients (including external recipients) disclosing non-confidential or non-personal information	Integrity	Moderate
Information sent to an unauthorised recipient(s) containing confidential and sensitive personal information (whether Internal or External)	Integrity/Confidentiality	Major
Loss of equipment		
Loss or theft of equipment containing no confidential and/or personal information	Availability	Minor/ Moderate
Loss and theft of equipment containing confidential and/or personal information but with encryption software installed on the equipment	Availability/ Confidentiality	Moderate
Loss and theft of equipment containing confidential and/or sensitive personal information where equipment has no encryption software installed	Availability/ Confidentiality	Major
Inappropriate material found on PC	Accountability	Minor to Major depending on the type of material found on the PC
Illegal material found on PC	Accountability	Major
Inappropriate/unauthorised use of the network/software leading to a disruption of services	Availability	Major

Inappropriate use of the internet or email as defined within the AUP Policy	Accountability/ Availability	Minor to Major depending on the circumstances
Passwords written down leading to unauthorised access	Integrity/ Confidentiality/ Availability & Accountability	Moderate/ Major depending on the type of information and system and impact of the incident
Offensive emails being sent	Accountability	Moderate to Major depending on content of the
Spam or 'phishing' emails	Availability	Minor to Moderate depending on the impact and
Information sent externally or internally by fax, post or hand (containing no confidential or personal information) is lost	Availability	Moderate
Information sent externally or internally by personal information) is lost fax, post or hand (containing confidential or sensitive	Integrity/ Confidentiality/ Availability &	Major
Unintentional corruption of data	Availability	Moderate/Major depending on the amount of data
Intentional corruption of data	Availability and Accountability	Major
Password sharing	Accountability/ Integrity/ Confidentiality	Moderate to Major depending the type of data in question
Downloading or copying of unlicensed software	Accountability	Major
Information/data deleted or amended from a database in error	Accountability/ Integrity & Availability	Moderate
Information/data deleted or amended from a database maliciously	Accountability/ Integrity & Availability	Major
Confidential information disposed of inappropriately	Accountability	Major
Website Hacked	Availability/ Integrity	Moderate to Major depending on the criticality of the
Misuse of Telephony Service	Accountability	Minor to Major on the level of misuse

Dear Parents/Carers of

I am contacting you because it has come to my attention that there has been a breach in the security of Personal Information held about your child by Park Road Academy Primary School.

The circumstances of the incident are as follow:

Your child's completed health questionnaire from the school nurse was mistakenly sent to 11 other families in the Reception class. The personal data sent by mistake included:

- *Your child's name*
- *Your child's gender*
- *Your child's date of birth*
- *Your child's place of birth*
- *Your child's NHS number*
- *Your child's Home address*
- *Your Mobile telephone number*
- *Your Email address*
- *Your previous address*
- *Your child's previous school*
- *Name of your child's GP*
- *Your child's Immunisation record*
- *Details of your child's medical conditions.*
- *Your child's ethnicity and their home language.*

The breach was brought to our attention by our Clerical Assistant checking delivery status of email and noticing that the incorrect attachment had been included.

I can confirm that Park Road Academy take the security of the Personal Data we control very seriously and steps have been taken to minimize the risk of this incident reoccurring and to mitigate any implications this incident may have on you and your privacy.

The following steps have been taken to ensure this error has been contained and will not be repeated;

- The email was recalled as soon as possible.
- Recipients of data were contacted and asked to delete the email.
- The breach occurred because a completed health questionnaire was sent out to some parents instead of the blank template document. The two documents had the same file name.

- Email attachments will be double-checked prior to sending in future.
- We will ensure documents containing sensitive personal data are labelled and stored appropriately to prevent misuse.

I would like to take this opportunity to apologise on behalf of Park Road Academy for this incident and any inconvenience or undue concern it may have caused you. If you would like to discuss this matter prior to taking further action please do not hesitate to contact me on 0161 972 4820 or SRI@parkroadacademy.co.uk.

Should you wish to raise a formal complaint regarding this matter, you may do so by contacting the School's Senior Responsible Individual: Mrs S Breen (SRI@parkroadacademy.co.uk)

Yours sincerely

Mrs S Breen (Senior Responsible Individual)