




General Data Protection Regulations (GDPR)

Rise Park Primary and Nursery School

Data Incidents and Breaches Policy

Signed by Chair of Committee	
Print Name	Jeanette Kirkby
Date	March 2020
Date of review	March 2021

Dealing with Data Incidents and Breaches

This guide is designed to assist colleagues in dealing with and appropriately responding to data incidents.

1. Introduction

Under the General Data Protection Regulation and the Data Protection Act 2018 a personal data breach must be notified to the Information Commissioners Office (ICO), no later than 72 hours after becoming aware of a data breach (unless a breach is unlikely to result in a risk to the rights and freedoms of individuals) and in certain cases, communicate the breach to the individuals whose personal data have been affected by the breach. This procedure manual and guidance is to be read in conjunction with the Data Protection Policy and other relevant guidance. The manual describes the procedure to be followed by members of staff when they become aware of a data breach.

2. Duty to protect personal information

The school has a duty under the sixth principle of Article 5 of the General Data Protection Regulation (GDPR) and section 33 to 38 of the likely Data Protection Act 2018 to ensure that it takes appropriate technical and organisational measures to protect the personal information it holds against unauthorised or unlawful processing, accidental loss, misuse, destruction, and damage.

Despite robust policies, guidance and procedures being in place, occurrences of data incidents involving loss or inappropriate access may still occur due to human error, wilful wrongdoing or other unforeseen circumstances. This document sets out the procedure which should be followed when a data incident occurs and the expected action(s) to be taken by:

- the person reporting an incident
- the staff member[Data Protection Officer] dealing with the incident
- The Data Protection Officer who will report the matter to the ICO if it is a personal data breach

3. What is a data incident?

A **Data Incident** is a process failure where it appears personal data or information in any medium (paper, electronic, laptop, data stick, etc.), including verbal information, is:

- Sent, handed, or given verbally to someone who should not have access to it
 - Lost or stolen
 - Accessed inappropriately either intentionally or unintentionally
 - Transmitted insecurely or uploaded inappropriately to a webpage
 - Disposed of in an unsecure manner.
-

General Data Protection Regulation (GPDR)

Examples of data breaches in school include:

- A full sickness record mistakenly sent to new employer as part of a reference
- Sensitive personal data lost in the post - about a hearing to investigate complaints about exclusion from school
- Pupil personal data found at printer by another pupil
- Pupil reports sent to wrong address
- Email addressing - non-use of BCC where it would have been appropriate
- Text message re a pupil's behaviour intended for their parents sent to all parents
- Data file with staff and pupil personal data accidentally placed in shared drive
- Inappropriate disclosure of pupil's information to absent parent
- Sending Special (Sensitive) Personal Data via unprotected email
- Lost unprotected USB sticks including pupil data (academic progress)
- Unencrypted drives / laptops / devices stolen from staff homes / cars / bags
- School website hacked, administrator passwords stolen. The same password for website administrator access and access to the main school pupil database. Hackers access information from the database
- Spreadsheet uploaded to website containing full details of pupil premium spending
- Parent passwords to access child information not sufficiently strong
- Poor website security; personal data left accessible by inadequate technical safeguards, e.g. inaccurate coding, inadequate penetration testing, etc.

4. When is a data incident a breach, or a near miss or no breach?

A data incident only becomes a **Data Breach** if, upon investigation by the Data Protection Officer it is found that security is breached because sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so. The severity level of the data breach is determined by elements such as the number of individuals affected, the sensitivity of the information, containment of the incident, recovery of the data and assessment of on-going risk.

Investigation of a data incident can find that a **Near Miss** or **No Breach** has taken place. A **Near Miss** highlights areas at risk of data breaches, but is an event that did not actually result in a breach although it had the potential to do so. For examples an encrypted email containing personal information is sent in error to a partner organisation but no personal information can be accessed; personal information sent in error to colleague or a partner organisation but it is password protected; information is lost, but recovered without any of the contents being disclosed to anyone.

General Data Protection Regulation (GDPR)

8. What happens if the school fails to notify the Data Controller within 72 hours?

The ICO have the power to fine the school up to 2% of their turnover.

9. When does the School become aware that the data breach has occurred?

The school becomes aware when they have a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. This will depend on the circumstances of the breach. In some cases, it will become relatively clear from the outset that there has been a breach. In others, it may take some time to establish if personal data has been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached and if so, take remedial action and notify the ICO if required. Examples include:

- A parent informs the school that they received a text or letter about another pupil by mistake and shows staff the text which provides evidence of the unauthorised disclosure. As the school have been presented with clear evidence of a breach there can be no doubt when the school became aware.
- A teacher reports a loss of an unencrypted memory stick that contained personal information relating to a pupil at the school. In cases where a small, unencrypted device is lost, it is not normally possible to determine whether someone has gained unauthorised access to the data it contains. Consequently, an incident like this would need to be notified to the ICO as there is a reasonable degree of certainty that a breach has occurred and the school would become aware when the teacher first realised the memory stick was lost.

10. What information should be notified to the ICO?

- a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and (does this mean the same?) the types and approximate numbers of the personal data records concerned.
- b) Inform the ICO of the Data Protection Officer's details or other contact point where more information can be obtained
- c) Describe the likely consequences of the personal data breach
- d) Describe the measures taken or proposed to be taken by the school to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects.

General Data Protection Regulation (GDPR)

Data Protection Officer	<p>→ The Data Subjects will be notified when there is a high risk to the rights and freedoms of the individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data has been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals:</p> <ul style="list-style-type: none"> ○ Racial or Ethnic Origin ○ Political opinions, Religious or Philosophical beliefs ○ Trade Union Membership ○ Data concerning Health or Genetic Data ○ Data concerning Sex Life or Sexual Orientation ○ Criminal Conviction <p>Such damage should be considered likely to occur and therefore, data subjects should be notified as a matter of course.</p>	<p>→</p> <ul style="list-style-type: none"> • Informing data subjects of the incident, and if they are at risk due to the incident, giving clear advice on the steps they can take to protect themselves. • Informing the police where appropriate, e.g. where property is stolen, where fraudulent activity has taken place, an offence under the Computer Misuse Act or the GDPR has occurred.
--------------------------------	--	--

Flowchart - key steps for Data Protection Officer producing an action plan to reduce the likelihood of the incident recurring:

Action By		Immediate Action Required		Next Steps
Data Protection Officer	➔	<p>Once any immediate and urgent actions have been taken and the investigation into the incident has been carried out, an action plan needs to be drawn up which is designed to reduce the likelihood of a similar incident occurring again. Every incident is different and therefore the action plan drawn up will be unique to address the set of circumstances that led up to the incident. However, across all incidents there are a number of common contributory factors that can be addressed in a similar way, e.g. changes to procedures, raising awareness, etc.</p> <p>A list of actions to address these more common contributory factors is set out in Appendix 1. The DPO should ensure that any contributory factors that are specific and unique to a particular incident are addressed.</p>	➔	<ul style="list-style-type: none"> Details of agreed actions, deadlines, and evidence required will be kept by the DPO and any actions carried out by the relevant member of staff. Evidence that actions have been completed should be sent by the member of staff to the DPO.

Flowchart - key steps for Data Protection Officer monitoring an Action Plan until all actions have been completed:

Action By		Immediate Action Required		Next Steps
Data Protection Officer	➔	<p>The case remains open until all actions required to:</p> <ul style="list-style-type: none"> remediate the effects of the incident reduce the likelihood of a recurrence <p>are completed.</p>	➔	<p>Completion of actions will ensure the school is working as safely as possible thus reducing the risk of further incidents occurring.</p>

Appendix 1 – most frequently occurring data incidents

This table contains a list of the most frequent occurrences of data incidents, along with the remedial action to be taken and the evidence required to prove that the action has been completed.

The following advice should be provided to all school staff to remind them of the need to maintain security around personal/confidential information:

- All staff members should undertake Data Protection training at least annually.
- Ensure that personal information is kept secure: lock/turn off your screen when not in use, secure information in lockable cabinets, use passwords/encryption (e.g. Office 365 encryption, Cryptshare, etc.) to share personal information.
- Colleagues should only use school IT approved encrypted electronic devices for school business; this is particularly important if devices are mobile and taken off-site (i.e. laptops, mobile phones, etc.)
- Lockable bags should be used when colleagues need to transfer/transport hard copy information.
- Double-check your email/letter address (or have a colleague do this) before you sent it. Ensure that you have the correct address.

Data Incident	Remedial action	Evidence required
No established procedure on dealing with personal information, and/or procedure not properly documented, and/or colleagues not receiving adequate procedure training, and/or procedure not being followed.	Write procedure and train colleagues accordingly.	Copy of procedure. Email confirmation from manager that training has taken place.
Staff have not received (refresher) Data Protection training.	Undertake Data Protection training.	Copy of training certificate.
Staff knowingly, wilfully and wrongly accessed information (i.e. information not pertinent to their role, without line management approval, etc.)	Disciplinary action.	Email confirmation from line-manager that disciplinary action is being taken.

General Data Protection Regulation (GDPR)

Incorrect documents picked up or documents left behind on the printer/photocopier.	Wherever possible, staff should stay with the printer/photocopier whilst printing/copying is in progress and ensure that all hard copies are collected. Care should be taken that no other documents are accidentally picked up (i.e. documents left behind by another user). Ensure that it is included in the procedure.	Copy of procedure.
Devices stolen or misplaced.	Ensure the school encrypts all its computers and other devices wherever it is practicable to do. Make sure staff understand the importance of using encryption, password protection and storage devices correctly and securely. Ensure that it is included in the procedure. If a device is misplaced and later found at found e.g. at a pupils home, establish who has access to it and that it is secure whilst it awaits collection. Let IT Support and Police know of the loss/theft.	Copy of procedure. Correspondence from IT and Police.
<p>Inappropriate discussion of confidential case details with colleagues who are not involved in the case or with other 3rd parties.</p> <p>Confidential case discussion in a public area or open plan office.</p> <p>Inappropriate discussion a case with a parent of a pupil whilst other family members/carers or other parents are also present.</p>	<p>Ensure that staff are aware of the importance of keeping personal information personal, and that they are aware of:</p> <ul style="list-style-type: none"> what they can and cannot share with colleagues/agencies their surroundings when discussing a case (i.e. can they be overheard) the need to obtain the pupils/parent consent before discussing their personal information in front of their family members/carers. <p>Undertake Data Protection training.</p>	<p>Copy of procedure.</p> <p>Copy of training certificate.</p>

Appendix 2 - Breach Log for recording data incidents

The table form below provides a simple breach log for recording data breaches. It is sourced from the Information



Personal data security breach log

Organisation:

[illegible]