Data Protection Policy

December 2024

Data Incidents and Breaches

Contents

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 UK 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 UK General Data Protection Regulation (UK 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 Data Protection Officer

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, memory 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.

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 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 father
- 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 example 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.

An event where at first sight a data breach has occurred, but after investigation it proved not to be a breach is classed as **No Breach**, e.g.

- It was found the information was accessed legitimately

The controller is the body that determines the purpose and means of processing the data, e.g. if a School Nurse emailed pupils' medical details to an NHS colleague insecurely. In this case, the NHS would have authority as the data controller and would deal with the incident.

5. Reporting a data incident to the Data Protection Officer

Upon discovering a data incident staff should immediately notify the Data Protection Officer and take any steps necessary to reduce the impact of the incident:

- Complete without delay the Initial Breach Form to collect the facts surrounding the incident and send this to schoolsdpo@gloucestershire.gov.uk.
- Take any additional steps necessary to reduce the impact of the incident - for example getting information taken down from the internet, retrieving information sent to the wrong address etc.
- Where it is clear that there is a high risk to the rights of the pupil or other data subject affected, then they must also be notified, or a parent or carer for that pupil.
- Where it is unclear advice should be sought from the DPO as to whether affected individuals would need to be notified.

Any data loss or data misuse incident must be reported to the Data Protection Officer.

6. What is a personal data breach?

The General Data Protection Regulation describes a personal data breach as being *a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed*. This means that any breach of principle 6 (security) that contains personal data is likely to be a personal data breach. It is a type of security incident.

7. When should the Information Commissioner's Office (ICO) be notified of a data breach?

When there is a High risk to the rights and freedoms of the individuals affected.

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

The ICO have the power to fine or impose enforcement action on the school.

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.

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.

Appendix 1 - 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 Commissioner's Office (ICO) who require its service providers to use the form when reporting breaches.

Personal data security breach log

Organisation: | Date:

No.	**Your ref.**	**Details of breach**						**Consequences of breach**	**Measures taken/to be taken**			
		Date of breach	No. people affected	Nature of breach (choose most relevant)	Description of breach	How you became aware of breach	Description of data		All individuals informed?	Remedial action	Other Regulators informed	When did you first notify the ICO of the breach?