Policy reviewed: Summer 2023
Next review: Summer 2024

Richard Avenue Primary School

Personal Data Breach Policy

1 Introduction & Background

The General Data Protection Regulation (GDPR) defines a **personal data breach** as 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.

An incident, whether **confirmed** or **suspected**, is an event which may compromise the confidentiality, integrity or availability of systems or data, either **accidentally or deliberately**, and may cause damage to the school's information assets and/or reputation.

Examples of Information Incidents include (but are not limited to) -

- Loss or theft of a **paper** or **electronic** record, like a file of documents, letters or reports that contains personal or confidential data
- Documents or emails containing personal or confidential data sent to the wrong person [including other people who work for the school or partner agencies]
- Any failure of business process/es to include adequate security measures
- Documents containing personal or confidential data lost in transit
- Personal and confidential data sent electronically without adequate protection (e.g. encryption)
- Personal or confidential information that has been stored somewhere [e.g. on a desk, open shelf] where it can be seen by an unauthorised person
- A computer screen displaying personal or confidential information, or open to a source of such information, that has been left unattended and accessible to someone who does not have viewing rights
- Personal or confidential data disclosed over the telephone to an inappropriate person in error or deliberately
- Information made public in error e.g. research findings that inadvertently identify individuals, person-identifying information discussed outside of work etc
- Personal or confidential information is disposed of inappropriately e.g. other than in a confidential waste bin
- Accidental or inadvertent destruction of unique copies of personal or confidential information before its identified destruction date
- Suspicion that someone has accessed a database, filing system or other data source without authority or permission

Under Article 33 of GDPR, the School is required to:

- Notify the Information Commissioner's Office (**ICO**) as soon as possible and **no later than 72 hours** after becoming aware of a breach, ***unless it is unlikely to result in a risk to the rights and freedoms of the affected people.***
- Provide a **reason** for delay if initial notification is not within 72 hours (notification may be phased as further information emerges)
- Maintain a **documented record** of the breach

A **data processor** (anyone processing data on the School's behalf i.e. usually a **contractor)** must notify the School as soon as possible after becoming aware of a breach.

The notification to the ICO must include:

- The nature of the breach (**what** happened, and **how**?), including the categories and numbers of both the **data subjects** (the people whom the information is about) and the **records** (e.g. 14 care records about 9 pupils)
- The name and contact details of the School's **Data Protection Officer**
- The likely **consequences** of the breach
- The **measures** taken (or proposed) to address the breach and mitigate any possible adverse effects

Under Article 34 of GDPR, the School is also required to notify the data subjects **themselves** (the affected people) where there is likely to be a ***high*** **risk** to their rights and freedoms. The notification to the people must **at least** include:

- The name and contact details of the School's **Data Protection Officer**
- The likely **consequences** of the breach
- The **measures** taken (or proposed) to address the breach and mitigate any possible adverse effects

Under Article 82 of GDPR, any person who has suffered material or non-material damage from a data breach has the right to receive **compensation** from the School for the damage suffered, unless the School can **prove** it is not responsible.

Under Article 83, the ICO can impose **fines** of up to 20 million Euros or 2% of the School's turnover for a personal data breach.

2 Managing & Reporting an Information Incident

- The **Head Teacher** and **School Business Manager** are the School's lead officers for Data Protection

- The **Data Protection Officer** (DPO) is the School's resource for monitoring compliance with GDPR, advising on data protection obligations and acting as the contact point for both data subjects and the **ICO**.

- In the event of a personal data breach, the lead officers, with the support of the DPO, are responsible for making arrangements for the incident to be logged, managed and investigated, and ensuring the response to the incident is given the appropriate priority. The lead officers should:

    - ❖ complete the **Breach Reporting Template** (see **Appendix 2**)

    - ❖ email it to data.protection@sunderland.gov.uk, or notify the DPO via telephone 07769 672 633

The Head and SBM can delegate individual tasks to appropriate officers within the school where appropriate to do so. The key requirements are;

- **Containment** and **Recovery** action to be initiated immediately.
- All Personal Data Breaches are to be reported **immediately (or as soon as possible if outside school hours)** by notifying the Head and/or SBM.

This policy applies to **all staff** (*optional:* **, pupils)** and **contractors** at the school/academy. This includes teaching students, temporary, casual, agency staff, suppliers and data processors working for or on behalf of the school/academy.