# Data Breach Process

| | |
|---|---|
| **Date Approved by School** | **Sept 25** |
| **Statutory Policy** | **Strongly Recommended** |
| **Required on Website** | **No** |
| **Review Period** | **2 Years** |
| **Next Review Date** | **Sept 27** |
| **Reviewed by** | **DPO** |

## 1. Revision History

The below table provides the revision history for this document. Each revision has an associated date, issue number, and description of the changes and/or content. The document revisions appear in descending order, with the most-recent iteration appearing first in the table.

| Date | Version | Description | Author |
|---|---|---|---|
| 30/05/2024 | 01.e | 3rd review – updated SIMs to read Arbor | Sarah Burns Data2Action |
| 03/07/2023 | 0.d | 2nd review. Changes made to reflect procedural change for VDPO | Sarah Burns, Data2Action |
| 15/07/22 | 0.c | 1st Review no changes | Jacqui Ridley, BWCET |
| 09/07/2021 | 0.b | Final Version | Jacqui Ridley, BWCET |
| 18/05/2021 | 0.a | Initial Draft | Karen Latimer, Data2Action |

## 2. Document Approval

| | |
|---|---|
| **Document Name** | Data Breach Process |
| **Publication Date** | July 2024 |
| **Prepared by** | Sarah Burns, Data2Action |
| **Approval** (Name & Organization) | C. Spencer (Headteacher)<br>Highfield Community Primary School |

## 3. Introduction

This document sets out the requirements and process for identifying and managing a data breach within the Highfield Community Primary School (the School).

The School holds large amounts of personal and sensitive data, is responsible for safeguarding the data held and is legally bound under the UK GDPR and Data Protection Act 2018 to ensure the security and confidentiality of all personal information processed. These responsibilities also extend to other organisations working on behalf of the School.

The UK GDPR introduces for the first time a legal requirement for a breach of personal data to be reported to the ICO and, in certain cases, communicate the breach to the data subject(s) affected by the breach.

Principle 7 of the DPA 2018 states as follows:

*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information.*

Accordingly, this process is an essential part of the School's compliance with the UK GDPR and Principle 7. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by virtue of the School's Data Protection Policy.

This document is for information and use by all employees of the School, any associates, contractors or agency staff and third-party processors and describes what a data breach is, how to identify a breach, log it, report it and assess/ take any necessary remedial action.

Associated documents: Data Protection Policy, Information and Cyber Security Policy and Acceptable Use of IT Systems Policy.

## 4. What is a personal data breach?

The term "personal data breach" is defined in UK GDPR and means 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. In summary, there will be a personal data breach whenever any personal data is:

- lost
- destroyed
- corrupted
- disclosed
- someone accesses the data or passes it on without proper authorisation
- the data is made unavailable, for example, when it has been encrypted by ransomware

This includes breaches that are the result of both accidental and deliberate causes. As such, a personal data breach includes much more than just losing personal data and includes a wide range of issues affecting personal data.

## 5. Identifying a data breach

A data breach can have a range of adverse effects on individuals, which include:

- emotional distress
- physical damage
- material damage

Some personal data breaches may merely cause an inconvenience to the individual however, other breaches may significantly affect individuals. Therefore, an assessment of the risk and impact must be made on a case-by-case basis.

Data breaches can be categorised in the following well-known information security principles:

- **Confidentiality breach**: where there is an unauthorised or accidental disclosure of, or access to, personal data.

- **Availability breach**: where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

- **Integrity breach**: where there is an unauthorised or accidental alteration of personal data.

A breach can be all three at the same time, or any combination of these. Examples of data breaches include:

- access by or disclosure to an unauthorised third party (anyone, internal or external, not authorised to access the data, disclosing personal data to an unauthorised party e.g., meeting minutes)
- deliberate or accidental action (or inaction) by a controller (Highfield Primary) or processor (any 3rd party suppliers, including where data is stored in 3rd party software systems for example Arbor)
- sending personal data to an incorrect recipient (for example, via email, in the post, pupil school bags, parents evening, pupil reports)
- computing devices containing personal data being lost or stolen (homeworking/ laptops)
- alteration of personal data without permission and
- loss of availability of personal data.

Breaches often occur when computer equipment storing customer data is lost, shared or unlawfully used for non-authorised activity or whereby an authorised or unauthorised visitor has accessed the premises and is privy to personal data which may be visible on desks, computers, whiteboards etc. This is particularly important for anyone working off site, i.e. at home.

For further information on how to protect personal data, please refer to the Information and Cyber Security, Data Protection and Acceptable Use of IT Systems policies. If you are uncertain of how you can protect personal data, please discuss this with either your manager/ Headteacher or DPO.

Assessing the risks

When assessing risk to rights and freedoms of individuals, it is important to focus on the potential negative consequences for individuals. Recital 35 of the GDPR explains that:

*"A personal data breach may, if not addressed in an appropriate and timely manner, 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."*

## 6. What to do when a data breach is identified

**What to do when a data breach is identified?**

It is everyone's responsibility to identify and report a data breach and it is important to act quickly. The timeframe for reporting a data breach is **72 hours**, from the point the breach is first identified. During this limited period, a decision will need to be made by the School Director of Governance (in conjunction with the DPO) as to whether to notify the Information Commissioners Office (ICO) and the individual(s) concerned. If the breach is likely to result in a high risk or adversely affecting the impacted individuals' rights and freedoms, the individual(s) must also be informed without undue delay.

**All staff:**
In the first instance, upon identifying a data breach, you must **immediately:**

1. notify the Headteacher and log the breach details on the Virtual Data Protection Officer Portal (VDPO), note at this point it is critical the full facts are clearly understood, documented and cascaded.

**Headteacher:**

1. Promptly notify the School Director of Governance and DPO via email and follow up with a telephone call within the same working day.
2. Assess whether any immediate remedial action can be implemented to prevent any further breach or to mitigate the impact of the breach.
   Ensure the breach is recorded on the VDPO as this will create a necessary log.

**Director of Governance/ DPO:**

1. Collect all the known facts.
2. Assess the risks to the data subject.
3. Make an informed decision as to whether to notify the breach to the ICO and Data Subject(s).
4. Ensure immediate mitigating action is implemented.
5. Update the VDPO breach record as necessary
6. Undertake a root cause analysis and make recommendations to address any underlying issues.

The DPO will work with relevant personnel to help inform any decisions, provide guidance throughout the full breach process, be the interface with the ICO where appropriate and ensure all necessary data is logged appropriately.

Where the breach is not deemed as high risk to the rights and freedoms of individuals, the DPO may decide not to notify the ICO/ individuals concerned. Where this is the case, the breach must still be recorded on the VDPO and remedial actions taken as necessary.

All staff and any other relevant individuals collecting and processing personal data on behalf of the School will be notified at this point of any changes to processes because of a data breach which then must be adopted and adhered to.

## 7. What information should be provided in a breach notification to the ICO

When reporting a breach, a description of the nature of the personal data breach must be noted including:

- the categories and approximate number of individuals concerned.
- the categories and approximate number of personal data records concerned.
- the name and contact details of the data protection officer (where applicable) or other contact point where more information can be obtained.
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

## 8. What happens if we fail to notify the ICO/ Individuals concerned

Failing to notify a breach when required to do so can result in a significant fine of up to ***20 million euros or 4 per cent of the company's global turnover.*** The fine can be combined with the ICO's other corrective powers, it is therefore vital that everyone takes responsibility for identifying and reporting the breach internally and without delay.

ICO contact details:
Information Commissioner's Office
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Helpline number: 0303 123 111