Data Breach Response Plan

Seven Springs Education

Approved by:	Willow Hewitt	**Date:**	22/08/23
Last reviewed on:	22/08/23		
Next review due by:	02/11/23		

Contents

1. Introduction

This data breach response plan sits alongside our Seven Springs Education Data Protection Policy, which it should be read in conjunction with. If you have any queries, please contact Joyce Wong (Joyce@seven-springs.co.uk), our Data Protection Lead, in the first instance.

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."

A breach of personal data is a type of security incident and falls into one of three categories:

- "Confidentiality breach" - an unauthorised or accidental disclosure of, or access to, personal data
- "Integrity breach" - an unauthorised or accidental alteration of personal data
- "Availability breach" - an accidental or unauthorised loss of access to, or destruction of personal data.

A breach may concern the confidentiality, integrity and availability of personal data at the same time, or any combination. It can be the result of both accidental and deliberate causes.

Some examples of personal data breaches include:

- access by an unauthorised third party (including the malicious acts of hackers and scammers)
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing/mobile devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data, e.g. when it has been encrypted by ransomware, or accidentally lost or destroyed (including natural disasters such as fire and flood).

Under the GDPR, any breach of personal data requires mandatory notification to our supervisory authority, the Information Commissioner's Office (ICO), unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

2. When a Breach of Personal Data Occurs

As soon as we are aware* that a breach of personal data has occurred, we will immediately seek to contain the incident and also assess the risk to the rights and freedoms of the individual(s) involved.

*Awareness of a breach occurs when we have a reasonable degree of certainty that a breach has occurred.

The GDPR requires us to use our resources to ensure we are 'aware' of a data breach in a timely manner. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised.

A data incident/breach may occur during public holidays and out of office hours, when Seven Springs Education is closed or we have a reduced number of staff available. We will ensure that all members of staff have the contact details of the Data Protection Lead and DPO so that any incident/breach can still be dealt with appropriately. These contact details are also included in our Data Protection Policy and Privacy Notices, which are available on our website.

3. Assessment of Risk

The risk from a breach is assessed on a case-by-case basis, and both the severity of the potential impact on the rights and freedoms of the individuals and the likelihood will be considered.

When assessing the risk to individuals as a result of a personal data breach, we will consider:

- The type of breach
- The nature, sensitivity and volume of the personal data
- How easy it is to identify individuals
- The severity of consequences for individuals
- Special characteristics of the individual, e.g. if they are children
- Any special characteristics of our organisation
- The number of affected individuals.

A breach is likely to result in a risk to the rights and freedoms of individuals if it could result in physical, material or non-material (e.g. emotional) damage. In particular:

- Loss of control over personal data
- Limitation or deprivation of individuals' rights
- Discrimination
- Identity theft or fraud
- Financial loss
- Damage to reputation
- Unauthorised reversal of pseudonymisation
- Loss of confidentiality of personal data protected by professional secrecy
- Any other significant economic or social disadvantage.

Where special category data* is involved, the GDPR states that such damage should be considered to be likely to occur.

*Special category data is data that is considered more sensitive and requires greater protection: racial or ethnic origin, political opinion, religion or philosophical beliefs, trade union membership, genetic data, data concerning health or sex life, or biometric data used for identification purposes. Data relating to criminal convictions is afforded similar special protection.

4. Notification to the ICO

As a result of this assessment, if we believe that there is a risk to the rights and freedoms of the individual(s), we will notify the Information Commissioner's Office, as required under the GDPR. If we

are in any doubt, we will always err on the side of caution and notify the ICO.

Where we assess a breach is reportable to the ICO, we must make this report without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach.

As a minimum, we must include in our notification:

- description of the nature of the personal data breach including, where possible:
    - categories and approximate number of individuals concerned
    - categories and approximate number of personal data records concerned
- name and contact details of the DPO
- description of the likely consequences of the personal data breach
- description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

The GDPR makes no allowance in the statutory reporting timescale of 72 hours for breaches that occur during public holidays or out of office hours. Therefore, it is important that staff contact the organisation's Data Protection Lead and the DPO as soon as possible.

5. Communication to affected individuals

Where a data breach is likely to result in a high risk to the rights and freedoms of individuals, we will notify affected individuals as soon as possible. We will provide:

- A description of the nature of the breach
- The name and contact details of the DPO and/or Data Protection Lead
- A description of the likely consequences of the breach
- A description of the measures taken, or proposed to be taken, by the organisation to address the breach and mitigate any possible adverse effects.

We will also consider what specific advice we can provide to individuals to help them protect themselves, such as resetting passwords where access credentials have been compromised.

6. Roles and Responsibilities

All Staff - if any member of staff believes a breach of personal data has occurred, or might have occurred, they must immediately notify the Data Protection Lead (Joyce Wong, Joyce@seven-springs.co.uk), who will liaise with the Data Protection Officer:

Nicola Cook, SchoolsDPO Ltd: 01296 658502, nicola@schoolsdpo.com.

If members of staff receive personal data sent in error, they must alert the sender and the **Data Protection Lead** as soon as they become aware of the error.

The **Data Protection Lead**, with the support of colleagues, will investigate the report and determine

whether a breach has occurred. To decide, they will consider whether personal data has been accidentally or unlawfully:

- Lost
- Stolen
- Destroyed
- Altered
- Disclosed, or made available where it should not have been
- Made available to unauthorised people.

The **Data Protection Lead** will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.

In discussion with the **Data Protection Lead**, the **DPO** will assess the potential consequences of the breach and advise whether the breach needs to be reported to the ICO.

If the breach is likely to be a risk to the people's rights and freedoms, the **DPO** will notify the ICO.

Where a breach is likely to result in a high risk to people's rights and freedoms, the **Data Protection Lead** will promptly inform, in writing, all individuals whose personal data has been breached. This notification will include:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.

- The **Data Protection Lead** will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
- The **Data Protection Lead** will document each breach, irrespective of whether it is reported to the ICO, and ensure a record is kept in the Data Breach Register.

7. Actions to minimise the impact of data breaches

The type of action we might take will depend on the nature of the breach, but could include (this list is not exhaustive):

- Attempting to recover lost equipment
- Use of back-ups to restore lost/damaged/stolen data
- Changing entry codes or IT system passwords
- Attempting to recall emails containing personal information that are sent to unauthorised individuals
- Requesting personal data received in error is deleted and written confirmation is provided that the information has been deleted, and not shared, published, saved or replicated in any way
- Carrying out internet searches to check information hasn't been made public. If it has, asking the publisher/website owner/administrator to remove and destroy the information
- Briefing staff in case of phishing enquiries for further information on affected individuals

We will review the effectiveness of any actions taken and amend them as necessary after any data breach. This may include establishing more robust policies and procedures or providing further training for staff.

8. Accountability and Record-Keeping

We record all breaches of personal data regardless of whether they are reported to the ICO. This helps us demonstrate our compliance with the GDPR under its principle of accountability. It also ensures we have records should the ICO wish to see them.

Our data breach register includes:

- Summary of the facts:
    - including the types and amount of personal data involved
    - details of the cause of the breach and impact on the individuals whose data is involved
- Actions taken to contain the breach as well as mitigate its possible adverse effects
- Any actions taken to prevent future breaches.