The Stonehenge School - Data breach procedures and data breach incident form

Introduction

This document sets out the guidance and procedure for personal data breach incidents and must be read in conjunction with the School's Data Protection Policy

Purpose and scope

The purpose of this procedure is to provide a framework within which Stonehenge School will ensure compliance with the legislative requirements of managing a personal data breach incident, or suspected personal data breach incident.

This procedure applies to school staff, agency workers, students, volunteers, contractors and third party agents who process data for or on behalf of the school and it must be complied with in the event of a personal data breach.

Personal data breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure, theft, or unauthorised access, to personal data.

Examples of personal data breaches

- Loss or theft of personal data or equipment (encrypted and non-encrypted devices) on which personal data is stored, e.g. loss of paper record, laptop, iPad or USB stick
- Inappropriate access controls allowing unauthorised use, e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to personal data or information systems
- Equipment failure
- Human error, e.g. email containing personal data sent to the incorrect recipient
- Unauthorised disclosure of sensitive or confidential information, e.g. document posted to an incorrect address or addressee
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it
- Insecure disposal of paperwork containing personal data

Responding to a personal data breach

To comply with the GDPR legislative requirements Stonehenge School must:

- have in place a process to assess the likely risk to individuals as a result of a breach.
- know who the relevant supervisory authority for our processing activities is.
- have a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
- know what information we must give the ICO about a breach.
- have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.
- know we must inform affected individuals without undue delay.

- know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.
- keep a record of all security incidents involving personal data, even if they don't all need to be reported. Some of these incidents must be reported to the Information Commissioner within 72 hours of detection, and without undue delay to data subjects (individuals) affected by the incident. It is vital that all staff report a personal data breach, or suspected personal data breach, however minor, as soon as possible after discovery so that we can use the 72 hours to establish what has happened, the size of the breach and whether it needs to be reported further.

Why should breaches be reported?

The longer an incident goes unreported, the harder it gets to resolve any vulnerabilities allowing the incident to escalate or for further incidents to occur. Impacted individuals have a right to know that their data may have been compromised and that they could then take steps that could minimise an adverse impact on them such as informing their bank that their bank details have been compromised.

Without timely visibility of the incident through reporting the school may not be able to fulfil its legal obligations. The EU General Data Protection Regulations (GDPR) places a duty on organisations to report personal data breaches to the Information Commissioner's Office. If the breach is likely to have a significant detrimental effect on individuals (e.g. discrimination, damage to reputation, financial loss, loss of confidentiality or any significant economic or social damage) it must be reported **within 72 hours of becoming aware of the breach.**

Knowing that a breach has occurred and delaying reporting reduces the time available for the investigation team to understand and assist with a response and still meet privacy compliance requirements.

Understanding the cause of breaches allows us to develop and implement systems and processes that are more robust to prevent future breaches and protect personal data

Procedure for reporting a personal data breach incident

The primary point of contact for reporting a data breach incident is the School Data Protection Officer (DPO).

The DPO (or nominated deputy) will investigate the breach and, where appropriate, notify relevant line management and HR.

However the breach has occurred the following steps will be taken immediately:

1. **Internal notification:** Responsibility for reporting a suspected breach lies with the person who discovered the breach. Suspected personal data breach incidents should be reported immediately upon discovery, in writing (or by phone if that is not possible), to **the Data Protection Officer (DPO) at DPO@stonehenge.wilts.sch.uk, using the form found in Appendix A.** This form should be sent by email and copied to The Head Teacher (unless there is a need to report it confidentially to the DPO).

2. **Containment:** The DPO will identify any steps that can be taken to contain the data breach (e.g. isolating or closing the compromised section of network, finding a lost piece of equipment, changing access codes) and liaise with the appropriate parties to action these.

3. **Recovery:** The DPO will establish whether any steps can be taken to recover any losses and limit the damage the breach could cause (e.g. physical recovery of equipment, back up tapes to restore lost or damaged data)

4. **Assess the risks:** Before deciding on the next course of action, The DPO will assess the risks associated with the data breach giving consideration to the notifications required in Part B, (Breach Risk assessment) in Appendix A.

5. **Breach reporting – to the Information Commissioner's Office (ICO):** Following the risk assessment which identifies a reportable personal data breach, The DPO (or nominated deputy) will notify the ICO. If the breach is deemed significant, notification to the ICO will be within 72 hours. The DPO will contact the ICO using their security breach helpline on 0303 123 1113, option 3 (open Mon – Fri 9am-5pm) or the ICO data breach Notification form can be completed and emailed to casework@ico.org.uk.

6. **Breach reporting - notification to the individual:** The DPO must assess whether it is appropriate to notify the individual(s) whose data has been breached. Where the personal data breach, or suspected personal data breach, is likely to result in impacting the rights and freedoms of the individual the school shall notify the affected individual, without undue delay, in accordance with the DPO's (or nominated deputy's) recommendations.

7. **Evaluation:** The DPO should assess whether any changes need to be made to the school processes and procedures to ensure that a similar breach does not occur.

Enforcement

Failure to adhere to this procedure, delay in reporting the breach to the DPO and non-reporting of breaches, may result in disciplinary action in accordance with the School Staff Disciplinary Procedure.

Review

This procedure will be reviewed bi-annually or where significant changes have occurred.

If you have any questions about the data breach procedure, please contact our **data protection officer via e-mail on** dpo@stonehenge.wilts.sch.uk .

Appendix A

Data Breach incident Form

The staff member notifying the breach should complete as much of the form as the available information allows.

Part A: Breach information

When did the breach occur (or become known)?	
Which staff member was involved in the breach?	
Who was the breach reported to?	
Date of report	
Time of report	
Description of breach	

Initial containment activity	

Part B Breach Risk Assessment

What type of data is involved?	Hard copy: Yes/No Electronic Data: Yes/No
Is the data categorised as 'sensitive' within one of the following categories:	Racial or Ethnic origin: Yes/No Political opinions: Yes/No Religious or philosophical beliefs: Yes/No Trade Union membership: Yes/No Data concerning health or sex life and sexual orientation: Yes/No Genetic Data Yes/No Biometric Data Yes/No
Were any protective measures in place to secure the data (e.g. encryption):	Yes/No If yes please outline
What has happened to the data:	
What could the data tell a third party about the individual:	
Number of individuals affected by the breach:	
Whose data has been breached:	
What harm can come to those individuals	
Are their wider consequences to consider (e.g. reputational loss):	

Part C: Breach notification:

Is the breach likely to result in a risk to people's rights and freedoms?	Yes/No If Yes, then the ICO should be notified within 72 hours

Date ICO notified:	
Time ICO notified:	
Reported by:	
Method used to notify ICO:	
Notes:	
Is the breach likely to result in a high risk to people's rights and freedoms	Yes/No If Yes, then the individual should be notified
Date individual notified:	
Notified by:	
Notes:	

Part D: Breach Action Plan

Action to be taken to recover the data	
Relevant governors/trustees to be notified:	Names:
	Date notified:
Notification to any other relevant external agencies	External agencies:
	Date notified:
Internal procedures (e.g. disciplinary investigation) to be completed:	
Steps needed to prevent reoccurrence of breach:	