Star Primary School

Security Incident Procedure

Author: G Williams	Position: AHT	
Status: [Approved/Draft]		
Last Updated: Summer 2023	Next Review: Summer 2025	Version: 1.0

Table of Contents

1.0 Overview

The School maintains a robust and structured program for data compliance and monitoring. However, not all risks can be completely mitigated and security incidents may occur from time to time despite best endeavours.

The protection and security of the data that is processed by the School, including personal information, is of paramount importance to the School. Data specific controls and protocols have been developed for any breaches involving confidential information and personal data.

The purpose of this document is to describe the School's policy and procedure for data security incidents including the recording and reporting of personal data breaches.

2.0 Scope and Applicability

This procedure applies to all security incidents that occur within the school environment. This extends to remote working. Security incidents which occur in any of the Schools Processors are also included within this procedure.

All staff have a responsibility to identify and record any security incidents relating to the potential loss of School data. Therefore, this procedure is applicable to all staff involved with the running of the school including employees, contractors and agency staff.

The School's definition of a security incident for the purposes of this procedure is any breach of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to data.

3.0 General Procedure

The School captures all security incidents as it allows the School to understand areas of weakness and highlights changes that should be made to policies and procedures to ensure effectiveness.

Any security incidents that are found to include personal data must be treated in accordance with this procedure and the UK GDPR.

3.1 Identification of Incidents

The School's definition of a security incident for the purposes of this policy is any breach of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to data.

The recording of security incidents shall take place irrespective of how the incident occurred and who was responsible.

Prompt action may be necessary to reduce the potential impact of an incident, so there may be occasions when an incident is resolved before it is recorded. If this occurs, a breach incident form should be completed as soon as possible after the event.

Where a processor suffers a data breach, the processor will notify the School as soon without undue delay. The School is responsible for notifying the DPO and following all notification procedures in the same way that the School will deal with internal incidents.

3.2 Incident Reporting

The School will capture all security incidents as it allows the School to understand areas of weakness and highlights changes that should be made to policies and procedures to ensure effectiveness.

Any security incidents that are found to include personal data must be treated in accordance with this procedure and the data protection legislation.

Staff have been trained to identify a security incident and the procedure for reporting it.

As soon as a security incident has been identified, it must be reported immediately to the DPO so that breach procedures can be initiated and followed without undue delay.

The School is committed to complying with legislation without apportionment of blame.

It is important that every incident, however minor, is recorded and follows this procedure to ensure that the probability of reoccurrence is avoided or reduced, and the impact of future incidents is minimised.

3.3 Incident Investigation

Security Incidents can originate from human errors or system errors. The DPO will analyse recorded security incidents in order to ascertain whether or not personal data has been compromised. Each incident will be prioritised according to severity, which will be based upon the actual or potential impact of the incident upon and will be categorised as:

- Critical (C)
- High (H)
- Medium (M)
- Low (L)

For example, in the case of a 'Low' severity, 'no action' may be an acceptable option. In the case of a 'Critical' severity, the DPO will ascertain whether or not personal data has been compromised.

If personal data has not been compromised, the security incident will be referred to the Head Teacher for further consideration.

If personal data is found to have been compromised, the DPO will make recommendations to the School as to which immediate actions should be taken to mitigate the impact of the incident. Recommendations will also be made to prevent any future occurrence of the same root cause.

3.4 Personal Data Breach Notification

The DPO will review each personal data breach and will decide if notification to the Information Commissioner's Office (ICO) is required.

The ICO is to be notified of any personal data breach where it is likely to result in a risk to the rights and freedoms of individuals.

Affected Data Subjects are to be notified without undue delay of any personal data breach where it is also likely to result in a risk to the rights and freedoms of individuals. The DPO will provide guidance to the school as to the appropriate course of action.

3.5 Notification to the ICO

Where applicable, the DPO will notify the ICO of the personal data breach no later than 72 hours after the School becomes aware of the incident and are kept notified throughout any breach investigation. The ICO will be provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

The following information will be included in the notification to the ICO:

- A description of the nature of the personal data breach
- 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 DPO
- A description of the likely consequences of the personal data breach
- 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

The DPO will notify the ICO via telephone or the online reporting system.

Where the School does not have full information regarding the personal data breach, a partial report should be submitted to the ICO with subsequent reports to follow as information becomes available.

The ICO will provide the DPO with an acknowledgement of the notification. In due course the ICO will either request more information from the DPO or will advise the DPO of the outcome following their investigation. The DPO will keep the School abreast of all developments.

3.6 Data Subject Notification

Where applicable, the DPO will ask the School to notify data subjects of the personal data breach without undue delay. Data subjects will be provided with the following:

- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects

A full report will be provided in a written, clear and legible format.

3.7 Record Keeping

All records and notes taken during the identification, recording, investigation and notification of the security incident are recorded and authorised by the DPO and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed regularly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

4.0 Roles and Responsibilities

As Data Controller, the school is responsible for complying with all security incidents.

Each member of staff is responsible for reporting security incidents that they are aware of.

The School's Data Protection lead person is responsible for notifying the DPO of any security incidents as and when they occur.

5.0 Compliance

Compliance is mandatory and will be enforced for all employees, vendors and contractors.

Non compliance with this and other policies may be subject to disciplinary action, up to and including dismissal.

6.0 Risk Management

Risk management for the School is set out in the Risk Register.

7.0 References

None

8.0 Definitions

DPO - Data Protection Officer

ICO - The Information Commissioner's Office

9.0 Review

This policy will be reviewed and updated on a regular basis, not to exceed 24 months.