Security Incident Procedure

Author: M Spencer	Position: DHT	
Status: [Approved/Draft]	Approved by Governing Body date:	
Last Updated: May 2018	Next Review: May 2019	Version: 1.0

1 Overview

Star Primary 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 despite best endeavours.

The protection and security of the data that is processed by Star Primary 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 data that is subject to the General Data Protection Regulation (GDPR) and other data protection laws.

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

2 Responsibilities

This procedure applies to all School staff. This includes contractors, temporary staff, and third party users and pertains to security incidents, including any data breaches.

All staff are required to be aware of and to follow this procedure in the event of a security incident and for reporting any security incidents to the Data Protection Officer (DPO).

3 Security Incident Procedure

Star Primary 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 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 GDPR.

3.1 Identification of an Incident

All staff have a responsibility to identify and record any security incidents relating to the potential loss of School 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 times 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.

3.2 Incident Recording

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.

Star Primary 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.

**********[Insert school specific procedure e.g. Breach reporting form/GDPRiS System]

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 Star Primary 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.

3.4.1 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.

3.4.2 Data Subject Notification

Where applicable, the DPO will 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.

3.5 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 Compliance

All staff are expected to comply with the School's policies to the highest standards. If any School employee is found to have breached this policy, they may be subject to the School disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).