SIR FRANCIS HILL
PRIMARY SCHOOL

Bristol Drive

Lincoln

LN6 7UE

Security Incident Policy

October 2025

Policy Owner	Data Protection Officer (DPO)
Version Number	V3.0
Governing Body Committee	Resources Committee
Date Approved by Governors	22nd October 2025
Next Review Date	October 2026

Contents

Contents	Page 2
Introduction	Page 3
Aim	Page 3
Scope	Page 3
What is a Security Incident?	Page 3
Near Misses and Suspected Incidents	Page 4
Actions on Identifying A Security Incident	Page 4
Personal Data Breachers	Page 4
General Principles	Pages 4-5
Further Information	Page 5
Review	Page 5
Annex A – Personal Data Breach Report Form	Pages 6-8

Introduction

Sir Francis Hill Primary School (the school) has a statutory duty to meet its obligations as set out within data protection legislation with regard to responding to, notifying and recording of personal data breaches.

Aim

This policy aims to ensure that the school appropriately manages security incidents relating to school information and Information Communications Technology (ICT).

It supports the schools Information Security Policy.

Scope

The policy applies to:

- Information processed by the school or on behalf of the school by a third party;
- School owned or leased ICT such as PC's; laptops; notebooks; smart phones; software; services, storage media and network resources.

What is a Security Incident?

A security incident is any fact or event that results in the compromise, misuse, or loss of information, ICT, or ICT services.

A security incident can impact the confidentiality, integrity and or availability of information.

Examples of security incidents include:

- The loss or theft of information
- Unauthorised disclosure of, or access to, information
- Loss or theft of ICT, media or devices
- Physical security breaches
- Deliberate or accidental breach of security policy
- Insecure disposal of information or ICT
- Malicious software (malware) infection
- Website defacement
- Denial of service attack
- Social engineering e.g. a fraudulent attempt to gain access to information or ICT.

Near Misses and Suspected Incidents

A near miss is as any fact or event that has happened, or may have happened, but did not result in a security incident.

A suspected incident is where initial information is sparse and it may be uncertain whether an actual incident has taken place.

Actions on Identifying a Security Incident

As soon as you identify, or suspect, that a security incident has occurred you must take the following action:

- Consider immediate action to contain, rectify or minimise the impact of the security incident e.g. asking an unintended email recipient to permanently delete the email.
- Immediately report all security incidents impacting ICT immediately to the school ICT Management Service.
- Immediately report all security incidents to the Data Protection Officer or Senior Leadership Team.
- Complete the schools security incident reporting form which is at Annex A to this policy and send it to the Data Protection Officer or Senior Leadership Team.

Personal Data Breaches

A personal data breach is a security incident that involves personal data.

All personal data breaches must be recorded on a record of personal data breaches.

Personal data breaches attract specific reporting obligations set out in data protection legislation.

A personal data breach which is likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office (ICO) no later than 72 hours from the point the school becomes aware of the breach.

A personal data breach which is likely to result in a *high* risk to the rights and freedoms of individuals must be reported to the impacted individuals without undue delay.

Whether or not a breach meets either of these thresholds will be determined on a case-by-case basis as part of the security incident process. The final decision on reporting requirements is the responsibility of the schools Data Protection Officer.

General Principles

The school encourages an open and transparent reporting system. Individuals must report all security incidents accurately and without delay and offer support in any investigation.

Individuals must also report near misses, potential security incidents, and security weaknesses.

All reported security incidents will be recorded.

The school will investigate security incidents in a manner proportionate to the potential impact of the incident. Where a root cause is identified the school will consider corrective action to help prevent similar incidents occurring.

The approach to an incident will consider:

- The type of incident
- The type of information involved
- The level of personal data involved
- The impact or potential impact
- The source of the incident

All security incidents will be considered for onward reporting both internally and externally.

Further Information

For further information regarding security incidents within the school please contact:

Name:	Mr Neil Fish-Clark
Position:	Assistant Head Teacher / Data Protection Officer
Email:	dpo@sfh.lincs.sch.uk
Phone:	01522 520359

Further advice and information is available from the Information Commissioner's Office at www.ico.org.uk.

Review

This policy shall be reviewed annually.

Annex A – Personal Data Breach Report Form

Sir Francis Hill Primary School
Personal Data Breach Report Form

Contact Information	
Name of Reporter	
Job Role	
Contact Details	
Incident Summary	
Date and time of incident	
Date and time the school was made aware	
Please describe the incident and, if possible, why it happened.	
Please describe any factors that may have reduced the impact of the incident. **e.g. stolen laptop was encrypted; incorrect email recipient has confirmed permanent destruction of email.**	
Please indicate the type of information involved **(tick all that apply)**	**Personal data** ☐ This is any information relating to an identifiable person who can be directly or indirectly identified by it e.g. name, contact details, identification number, email address, location data or online identifier. **Special Categories of personal data** Personal data that relates to the following categories: Race ☐ Ethnic origin ☐ Religious or philosophical beliefs ☐ Trade Union membership ☐ Sex life ☐ Sexual orientation ☐ Political opinions ☐ Physical or mental health or condition ☐ Genetic data ☐ Biometric data ☐ Criminal convictions or offences ☐ **Other sensitive information** ☐ This is information that does not contain personal data but which could have a negative impact on the school e.g. commercial, legal, or financial data. **Routine information** ☐ Information which is not sensitive and that will not have a negative impact on the school if it was compromised e.g. promotional leaflets.

If personal data is involved, what type of individual does the data relate to?	**Staff** ☐ **Pupil (Child)** ☐ **Parent** ☐ **Governor** ☐ **Other** ☐ (Please explain other here) **Not yet known** ☐
Immediate Action	
What immediate action has been taken in response to the incident? ***Consider actions to stop the breach and actions to prevent a similar incident happening again.***	
Impact on Affected Individual(s)	
What are the potential consequences for affected individuals? **For each consequence, please select the likelihood of it occurring.**	

	N/A	Unlikely	Likely	Almost Certain or Confirmed
Personal Safety	☐	☐	☐	☐
Safeguarding	☐	☐	☐	☐
Distress	☐	☐	☐	☐
Embarrassment	☐	☐	☐	☐
Interruption to services	☐	☐	☐	☐
Identity theft	☐	☐	☐	☐
Fraud	☐	☐	☐	☐
Financial Loss	☐	☐	☐	☐
Physical Harm	☐	☐	☐	☐
Reputational Damage	☐	☐	☐	☐
Discrimination	☐	☐	☐	☐
Other (provide details)	☐	☐	☐	☐

If personal data is involved, how many individuals could be affected?	
Please describe the potential impact to the school and/or partners and stakeholders. ***Consider the following areas:*** • ***Finance*** • ***Reputation*** • ***Delivery of education or related service*** • ***Legal and regulatory obligations*** • ***Other (please provide details)***	

Reporting	
Who, internally, has been advised of the incident? **Please include names and position.**	
Who, externally, has been advised of the incident **e.g. Partners, Police.**	
If personal data is involved, have the affected individual(s) been notified? **If yes, please also confirm when they were notified and by whom.** **If no, please explain why.**	
Further Information	
If you have any other information which is useful to the incident report please provide details here.	

Please email the report to the school's Data Protection Officer.
Email: dpo@sfh.lincs.sch.uk