CHIPPING SODBURY SCHOOL

Information Security Incident Procedure

Signed (chair): Robert Owen	Name: Robert Owen	Date: 15/5/2018
Signed (Head): Katherine Turner	Name: Katherine Turner	Date: 15/5/2018
Ratified by: Governing Body on 15/5/2018		Next Review: May 2020

Version 20171201

Table of Contents

1.Introduction

Chipping Sodbury School holds a large amount of personal and sensitive data. Every care must be taken by all staff to protect all personal and sensitive data. In the event that data is lost or shared inappropriately (actual or suspected) the school will take appropriate action to minimise any associated risks, both to the school and the Information owner and all incidents are to be reported to the headteacher, investigated thoroughly, and where appropriate the incidents will be reported to the Data Protection Officer and the Information Commissioner (ICO).

The loss or inappropriate sharing of data, whether actual or suspected is referred to in this Procedure as an “Information Security Incident” (“ISI”).

2 Purpose

This Procedure sets out the steps to be taken by all school employees if they become aware of or suspect an ISI has occurred.

For the purpose of this Procedure “employee” includes individuals employed on a permanent or temporary basis, or individuals engaged via agency arrangements, or individuals acting as consultants or agents of the school.

All employees however employed or engaged are under an obligation to report an ISI in accordance with this procedure.

The Procedure also applies to members of the Governing Body.

3 Scope

This Procedure applies to all personal and sensitive data held by the school.

4 Legal Context

The General Data Protection Regulation makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use, or disclosure of such information.

Article 5 of the General Data Protection Regulation states that organisations which process personal data must process data:

“in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”

Every employee, governor, contractor or agent acting with the authority of the school who use or who have access to personal information is required to comply with the General Data Protection Regulation and the Freedom of Information Act 2000 and with the requirements of this Procedure.

5 Other Relevant Policies/Procedures

This Procedure should be read in conjunction with the following policies/procedures in force at the time of the incident

ICT Security Policy
Data Protection Policy
Freedom of Information Policy
The Employee Code of Conduct
Managing Employee Performance

And any other policy relevant to the ISI in force at the date of the incident.

The inappropriate disclosure of information or a breach of the GDPR may result in disciplinary action which could result in dismissal.

Failure to act appropriately on becoming aware of an ISI may also result in disciplinary action.

6 Definition of an Information Security Incident

An ISI is any action that may compromise the confidentiality, integrity (i.e. accuracy or completeness), or availability of information; sometimes referred to as a 'data breach'. This includes both information stored and processed electronically and information stored in other forms, such as on paper, files, microfiche or removable devices e.g. memory sticks mobile phones, laptops, tablets or a verbal disclosure of data.

7 Types of Breach

An ISI includes, but is not restricted to, the following:

• the loss or theft of data or equipment on which data / information is stored;
• inappropriate access controls allowing unauthorised access;
• the transfer of data / information to those who are not entitled to receive it (including verbal disclosure);
• human error;
• attempts (either failed or successful) to gain unauthorised access to data/information storage or a computer system ("hacking");
• unauthorised changes to data / information or system hardware, or software;
• the unauthorised use of a system for the processing / storage of data by any person;
• a virus infection (unexpected or unusual behaviour of the workstation could indicate a virus infection);
• Business Continuity event, e.g. fire or flood.

8 What are the risks to the school from Information Security Incidents?

Compromise of information confidentiality, integrity, or availability could result in: reputational damage, detrimental effect on service provision, harm to individual(s), legislative non-compliance, and/or financial costs.

This Procedure aims to mitigate these risks by ensuring:

• all employees, governors, partners, contractors and third party users are aware of the procedure for reporting ISI's and their responsibility to promptly report any observed or suspected incident, or information security concern;

• reported incidents or concerns are promptly followed up in accordance with this Procedure;

• that following recovery from the information security incident existing controls are examined to determine their adequacy, and corrective action is taken to minimise the risk of similar incidents occurring;

• there are mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified, monitored, and reported.

9 Procedure Review

This procedure will be reviewed in line with the school's Data Protection Policy every two years.

10 Reporting an Information Security Incident concern

The school encourages open, honest and accurate reporting to minimise impact, improve practice and reduce risk.

ISI's must be reported without delay to the Headteacher, or governing body who will then appoint an Investigating Officer (IO).

In appointing an investigator careful consideration must be given to the expertise required in understanding the risk and impact of the incident.

11 Role of the Data Protection Officer

Article 39 of the GDPR sets a number of mandatory tasks for the DPO, but does not prevent further tasks being allocated, if appropriate.

Of particular relevance to breach notifications, tasks of DPOs include cooperating with the supervisory authority (the Information Commissioners Office in the UK) and the data subjects. It should also be noted that, when notifying the data breach to the ICO, Article 33(3)(b) requires the controller to provide the name and contact details of its DPO. These factors mean that the DPO will play an important role when

notifying a breach and during any subsequent investigation by the supervisory authority (the ICO in this country).

The DPO will work closely with the Investigating Officer.

The DPO will upon notification record the Security Incident in the Breach Log

The DPO or Investigating Officer must immediately:

• take appropriate steps to identify the nature and extent of the lost information and agree/take all necessary steps to recover any losses i.e. containment & recovery and limit any further damage. Where appropriate a risk assessment should be undertaken and be documented identifying agreed outcomes with reasons.
• identify if the information security incident concerns an IT system. If so they shall take immediate steps to notify IT of the incident
• consider at this stage whether the police need to be informed. This would be appropriate where illegal activity is known or suspected to have occurred e.g. theft, or where there is a risk that illegal activity might occur in the future.
• inform Strategic Communications about the ISI, so they can effectively manage any press enquiries
• if the breach may include the loss of bank details notify Financial Services, bank(s) etc of the potential loss so as to prevent fraudulent uses
• notify relevant staff groups of loss
• notify other relevant Local Authority departments as appropriate so as to minimise any exposure to risk, this is particularly important if the ISI relates to an attack on the school's ICT systems
• notify the School's Risk and Insurance Officer.
• obtain advice from HR as to the appropriateness of commencing processes in accordance with the Managing Employee Performance Procedure, and if so identify the appropriate lead officer.

All decisions taken and the responsibility for their discharge must be documented and be retained by the DPO in a decision log which is incorporated into the investigation report.

12 Investigating an information security incident (ISI)

The Investigation Officer (IO) shall immediately commence a comprehensive investigation of the ISI.

The IO should consider the type of data, its sensitivity, what protections are in place (eg encryption), what has happened to the data, how it could be used, how many people are affected by its loss, what type of people have been affected (e.g. pupils, staff, public, suppliers,) including their vulnerability and whether, and if so, what are the wider consequences of the breach.

Time is of the essence and, as such, there is a requirement for all investigation to be carried out expeditiously. It is imperative that on notification the DPO along with the IO identify all/any appropriate steps that need to be taken to minimise the impact of the breach. This includes the consideration of how the breach can be recovered and or contained. All agreed actions must be recorded and actioned without delay.

Timescales from realisation of incident	
Notification of incident to the head teacher or governing body	Without any delay. Immediate consideration by the HT/GB and recording of actions agreed concerning recovery/containment of the breach
Allocation by HT/GB to Investigating Officer	Without delay
Draft report to DPO (Phase 1 investigation)	As soon as possible but in any case well within 72 hours
Final report (to include completion of Phases 2 & 3)	Within 72 hours unless ICO already notified Further time extensions allowed by ICO for complex cases once notified.

13 Investigation Process

An Investigation falls in to 3 phases:

Phase 1

Immediately establishing/gathering the facts – how, what, why, when and who is affected. This element is time critical. The IO will need as a minimum to establish the following:

• When the incident occurred (a detailed chronology should be prepared).
• When was the data last seen and when was the loss realised (Dates and times)?
• Who was notified of the incident and when, establish how/when they become aware of, or suspected the incident?
• What & whose data has been lost/disclosed, are there any specific issues to be considered – e.g. vulnerability?
• How the loss/disclosure happened/why it happened?
• Where the incident occurred (school, other workplace, home, or public place)?
• How many data subjects information was disclosed?
• Who received the information?
• What is the potential impact on the data subject(s)?
• Was the data subject advised of the disclosure, should they be?
• Assess the risk faced by the individual's whose data has been compromised and how these risks should be managed.
• What was the format of the data (paper, electronic, removable devices)?
• Review any agreed actions taken relating to containment and recovery of the data and determine what, if any further action is required to be taken.

Following the completion of Phase 1 the IO and DPO should assess the Risk Assessment Scoring Matrix and based on the information now available the DPO should review all decisions taken in accordance with Section 11 above – Role of the DPO and revise accordingly.

Any revisions to the actions/decision must be recorded as part of the IO's report and the DPO should update the original decision log.

The DPO shall also determine at this stage whether the ISI requires notification to the ICO and/or other agencies. The decision taken and reasons shall be recorded in the breach log.

Details of the requirements for Notification are set out in Section15 below.

Phase 2

Assessing potential risks and identifying failures/shortcomings in procedures – what can be done to avoid/minimise the same/similar breach occurring in the future. Issues to be considered by the school will include:

• Was the person who made the disclosure authorised to have access to the data?
• Was the recipient authorised to access this type of data?
• Are there any existing procedures, are they sufficient?
• Were internal procedures followed, if not why not?
• What risks does the school face as a result of the breach?
• Identify all relevant staff training and guidance and establish whether individuals have undertaken all required training.

Phase 3

Developing an Improvement Plan, issues to consider will include:

• Identifying areas for improving systems, processes so as to minimise a repeat of the breach,
• Requirements for training,
• Identifiable breaches of adopted school policies

The draft report should be submitted to the DPO immediately on the completion of Phase 1. Submission should not be delayed pending the completion of an Improvement Plan.

The DPO will provide a quality assurance role and ensure that the breach log is updated at relevant intervals.

14 Submission of Final Report including Improvement Plan

It is critical to ensure the school improves its handling and management of data and as such the preparation of an Improvement Plan following an investigation is an important factor.

The IO should immediately following the completion of Phases 2 & 3 of the investigation prepare a draft Improvement Plan and send this to the DPO.

The Final Improvement Plan should include any comments made by the DPO in respect of the Improvement Plan, i.e. whether it is accepted or accepted subject to amendments.

The responsibility for the implementation of the Improvement Plan rests with the school.

15 Notification

The DPO will, in conjunction with the IO, at all relevant stages following the identification of an ISI, and in particular immediately after the conclusion of Phase 1 of the investigation, determine whether any further action is required, in particular whether any third parties should be notified of the ISI. The DPO shall record all decisions taken with reasons.

Following the completion of the IO's report the school shall consider whether any HR procedures should be commenced.

In the case of significant breaches the Information Commissioners Office will be notified within 72 hours. Consideration will be given to this by the DPO when the data loss/ breach is identified and at all appropriate stages thereafter during the investigation process.

The IO is required to make an assessment of the risks as part of the investigation. This assessment will be reviewed by the DPO following the completion of Phase 1 of the investigation. The criteria for reporting a matter to the ICO is outlined in Article 33 of the GDPR.

Other notifications may include the affected individuals and/or any external agencies, if any loss includes third party information.

The governing body will receive an annual report on data governance generally; this will also include details of any data breaches.

16 Retention of Data Breach reports

Each investigation and its results must be fully documented by the Investigating Officer and Data Protection Officer using the report form and any documentation retained for 6 years from the date the investigation was closed.

Appendix 1 ISI Reporting and Investigation Form

INFORMATION SECURITY INCIDENT

Reporting & Investigation Form

Introduction
This report has been developed to assist the Investigating Officer investigate information security incidents. Further information is available from the Data Breach Procedure

The report is broken into four phases as follows.

Phase			***Completed by***	***Timescale***
1.	**Recovery and containment**	Gathering initial information about the incident, the data involved and steps taken to recover and contain it	Investigating Officer	As soon as possible and **within 72 hours**
2.	**Investigation plan**	Initial risk assessment undertaken and consider who will undertake further investigation	Data Protection Officer	
3.	**Investigation**	Consider what happened against what should have happened. Review related guidance, policies and procedures as well as training needs. Identify any actions to mitigate against future incidents	Investigating Officer with support from the Data Protection Officer	By 10th working day
4.	**Review**	Consider investigation report, provide comment and identify possible further actions	Headteacher/ Governing Body	By 20th working day

PHASE ONE: Recovery and Containment

1. About the incident	
Date and time of incident	
Where did the incident occur?	
Date of notification to HT/GB	*If there was any delay in reporting the incident please explain why this was*
Who notified us of the incident?	
Please describe the incident in as much detail as possible, including dates; what happened, when, how and why? *Include initials of names of staff and data subjects so the IO can fully understand what has happened. Identifying information will be anonymised for any reporting purposes.*	

2. Has the data been recovered? This should be taken as soon as possible following notification
Please provide details of <u>how</u> you recovered the data and <u>when</u>. *Consider collecting any data that has been accidentally 'lost' rather than getting an unintended recipient to dispose of it.* What have you done to contain the incident? *For example, limiting the initial damage / notifying the Police of theft or providing support to safeguard data subjects involved*

3. **Type of Incident** mark "x" in all relevant categories							
Physical damage		Theft		Loss or Mislaid		Hacking	
Software Failure/ Systems Crash		Unauthorised presence / access		Break-in		Disclosure to known recipients	
Disclosure to unknown recipients		Other (Please state)					

4. **About the people affected (the data subjects)**	
How many individuals' data has been disclosed?	
Are the affected individuals aware that the incident has occurred? *If yes, what was their reaction?*	
When were they told?	
If you decided not to notify them please explain why not?	
Are there any potential consequences and adverse effects on those individuals? Are there any further steps needed to minimise / mitigate the effect on the affected individuals? If so, please provide details.	
Have any affected individuals complained about the incident?	

5. **Who has completed this form?**	
Names of people completing this form with job titles	
Date of completion	

PHASE TWO: Investigation Plan

6. **Risk Assessment Scoring Matrix** Using the matrix assess the risk. Sum up your risk assessment in the table in section 7.

How many people's personal information is at risk?	**Number of data subjects affected**	**Score**
	0-10	0
	11-100	1
	101-1,000	2
	1,000 – or more	3

Sensitivity Factors – select each that apply, weighing up the risks		**Score**
LOW	a) No sensitive personal data (as defined by GDPR) at risk nor data to which a duty of confidence is owed	-1
	b) Information readily accessible or already in the public domain or would be made available under access to information legislation e.g. FOI Act 2000	-1
	c) Information unlikely to identify individual(s)	-1
HIGH	d) Detailed information at risk e.g. SEND case notes, social care notes	+1
	e) High risk confidential information	+1
	f) One or more previous incidents of a similar type in the past 12 months	+1
	g) Failure to implement, enforce or follow appropriate organisational or technical safeguards to protect information	+1
	h) Likely to attract media interest and/or a complaint has been made directly to the ICO by a member of the public, another organisation or an individual	+1
	i) Individuals affected are likely to suffer substantial damage or distress, including significant embarrassment or detriment	+1
	j) Individuals affected are likely to have been placed at risk of or incurred physical harm or a clinical untoward incident	+1

7. **Risk Assessment Scoring**

Provide reasons if need be for your scores here	Date:	Score:
	Reasoning:	
	Date:	Score:
	Reasoning:	

8. **Others notified about incident**		
Name	**Title**	**Date**
	HR?	
	IT?	
	Legal	
	Risk & Insurance Services?	
	Police? Crime ref:	
	Third party?	

9. **Investigation plan**	
Name of Investigator	Date passed for further investigation
Any other details about investigation e.g. type of investigation	

PHASE THREE: Investigation

10. **Understanding what data security measures are currently in place**
What organisational / technical measures were in place to prevent an incident of this nature occurring?
Provide extracts from relevant policies, procedures or guidance that set out what should have happened.
Were appropriate security guidelines being followed? If not explain why.
11. **Training and communication** This section is about whether staff understood what organisational and technical data security measures were in place
Please confirm what data protection training staff have undertaken and when
What evidence is there to communicate the process to be followed? *For example, email reminders or operational procedure manual issued at team meeting.*

12. **Action plan** This section identifies any improvements to reduce the risk of a reoccurrence. This is also the place to record how lessons learned can be shared with colleagues.

Describe actions already or still to be taken to prevent a recurrence of this incident?

	Action required	***By whom?***	***By when?***
1.			
2.			
3.			
4.			
5.			
6.			

PHASE FOUR: Review

13. **Review undertaken**	
Name and title of Reviewer	Date of review
Comments	
Further Actions	