

Procedures for Reporting Handling Security Incidents

Updated: April 2021

Approved by Trustees: June 2021

Review date: April 2021

Reviewing Panel: Standards, staffing and curriculum (SSC)

Contents

1. Introduction.....	3
2. Quick Reference Guide to activities for managing security incidents	3
3. Policy References	4
4. Procedures.....	4
4.1. <i>What is a Security Incident?</i>	4
4.2. <i>Employee Responsibilities</i>	5
4.3. <i>Investigations</i>	5
4.4. <i>Timescales</i>	5
4.5. <i>Reporting to the ICO</i>	5
5. Advice and Support	6
6. Breach Statement.....	7
Appendix A: Risk Classification	7
Appendix B: Incident Types	8

1. Introduction

- 1.1. This document applies to everyone who undertakes duties on our behalf (including third parties, suppliers, partners and contractors etc.). We have a duty to ensure that the information we process and hold is secure. We will react appropriately to any actual or suspected security incidents relating to information, systems and data.
- 1.2. We recognise there are risks associated with individuals accessing and handling information in order to conduct our business and have in place Policy and Procedures which need to be followed. Security incidents occur when those policies are not followed. Therefore there is a need to report these incidents to manage the risks and identify improvements to decrease the number of future incidents.
- 1.3. Where an external supplier has reported a security incident it is the responsibility of the school to report the incident.

2. Quick Reference Guide to activities for managing security incidents

- Use the Outcome Report template to gather basic information about:
 - what has happened
 - who is involved
 - what has been done to manage the incident already

- From this information, classify the Security Incident using the criteria at [Appendix A](#)

If the risk scoring works out at 3 or more, then escalate to the incident investigator providing the Outcome report

- Ensure the investigator and SIRO are involved in investigating major/critical and escalated incidents and collect evidence as required
- Ensure remedial action is taken within 24 hours to recover unlawful disclosure of personal/ sensitive information
- Provide advice, support and intervention as appropriate to each case
- Inform data subjects (parents/ guardians, employees) if necessary
- Identify and manage consequent risks of the incident
- Identify expected outcomes, stakeholders and any policies or standards that may have been breached.
- Complete the Incident Outcome Report ([Appendix C](#)) and update your B1 reporting template.
- Following receipt of Outcome Reports analyse results looking at lessons learnt and implement required actions

- All outcome forms with actions that have future completion dates can be closed with a scheduled task created to review
- Preserve evidence and maintain an audit trail of events and evidence supporting decisions taken in response to the incident
- Retain records of all incidents as evidence of the how the process works
- Develop and implement an appropriate means of preventing similar incidents in the future

3. Policy References

3.1. This procedure is a requirement of the following policies:

- Security Incident Policy

4. Procedures

4.1. *What is a Security Incident?*

4.1.2 An **information security incident** is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information and weaken or impair business operations.

4.2.2 An **information security event** indicates that the security of an information system, service, or network may have been breached or compromised. An information security event indicates that an information security policy may have been violated or a safeguard may have failed.

4.3.2 See [Appendix B: Incident Types](#) for a comprehensive list of what is considered a breach. There are some examples below:

- Using, or being asked to use, another person's login or password (or both)
- Not locking your PC/ laptop before leaving it, if you are logged in;
- Allowing confidential information to be passed on to people who do not have the correct authorisation to see it or not preventing this;
- Sending personal information to the wrong recipient, either by email or post;
- Stolen or lost electronic equipment, including laptops or mobile phones;
- Sending abusive emails, or forwarding racist or sexist jokes or emails;
- Allowing someone to enter the building without an appropriate security checks, e.g. signing in process;

- Intentional or accidental infection of computer viruses or unauthorised software.

4.2. Employee Responsibilities

4.1.2 Anyone discovering a security incident, even those they think are minor, must immediately report it to the school office.

3.2.2. No retaliatory action will be taken against any member of staff who reports a security incident about another member of staff in good faith, regardless of the seriousness of the security incident or the level of individual responsible for the breach. Identification of a reporting party who requests anonymity shall be protected to the degree feasible, but cannot be guaranteed.

4.3. Investigations

4.1.2 The Headteacher or school information champion will classify the security incident using the scoring system at [Appendix A](#), and an investigator will be assigned. The Headteacher will oversee all major incidents to ensure they can assess and recommend a report to the Data Protection Officer (DPO) for the matter to be considered for notification to the ICO if required.

4.4. Timescales

4.1.2 The assigned incident investigator will contact those involved within 4 working hours of being notified of the incident, and will agree initial actions to be taken. Depending on the complexity of the incidents the timescales for completing investigations will vary. Security Incident Classifications can be found in [Appendix A](#). However, listed below are the expected timescales for the majority of incidents to be investigated and closed:

- **Minor/Near Miss (Scale = 1)** – closure within 1 week
- **Medium (Scale = 2)** – corrective action within 24 hours, investigation of cause of incident, implement preventative action and outcome report within 2 weeks
- **Major/Critical (Scale = 3)** – corrective action within 24 hours; investigation of cause to begin immediately and implement preventative action, including recommendations to Governors/Trust and outcome report to be completed within 1 month. Notification of major incidents requiring assessment for ICO notification must be sent to the DPO within 24 hours of becoming aware of the incident.

4.5. Reporting to the ICO

4.1.2 The Information Commissioner requires major breaches of Data Protection law to be reported within a statutory timescale. Your DPO will assess the need for notification according to the threshold dictated by the ICO.

4.2.2 It is the Senior Information Risk Owner's (SIRO) responsibility to decide whether to report a breach to the regulator; the Information Commissioner's Office (ICO) after consultation with the DPO.

4.3.2 The ICO state that they require notification of breaches where the incident "is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage". Each case must be assessed on a case by case basis and should involve the opinion of the DPO.

4.4.2 If the breach is considered to represent a 'high risk' to the data subject rights (i.e. it is a higher level of risk still than that requiring reporting to the ICO), then there is a further requirement that the data subjects themselves are formally notified by the School. The opinion of the DPO should be taken into account by the SIRO.

4.5.2 If the ICO is to be notified about the breach, the notification must contain:

- The nature of the breach including the categories and approximate number of the:
 - individuals concerned
 - personal data records concerned
- The name and contact details of the DPO or other contact point where more information can be obtained
- 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
- The measures taken to mitigate any possible adverse effects.

4.6.2 A notifiable breach has to be reported to the ICO under the GDPR within 72 hours of the School becoming aware of it. The law recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases; however the initial notification – if it is necessary to notify - must happen within the timescale.

4.7.2 If the breach is sufficiently serious to warrant notification to the public, the School must do so without delay.

4.8.2 The reasons behind the SIRO's decision whether or not to notify must be documented on the Security Incident Outcome Report Form and must include consideration of the DPO's opinion.

5. Advice and Support

5.1. If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact your SIRO.

6. Breach Statement

6.1. A breach of this procedure is a breach of Information Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendix A: Risk Classification

Any incident scoring 3 would be reportable to the SIRO and DPO for consideration of further reporting to the ICO, if it scores less, it is not. If in doubt please refer to SIRO for a decision.

1. *As defined by Data Protection Law, is the data:*

- Special Category (Sensitive) [1]
- Personal [0]

2. *Has the law been breached?*

- Yes [1]
- No [0]

3. *Did the data get sent:*

- Within the school [0]
- To an external partner organisation, e.g. NHS/ Social Care [1]
- To an external organisation/ individual [2]

4. Has the school applied the appropriate technical security (e.g. is the information encrypted, appropriate access controls in place, correct procedure followed):

- Yes [0]
- No [1]

Appendix B: Incident Types

The following is a list of security incident types which fall within the scope of the Policy and this Procedure:

Categories:	Description:	Incident Types:	Description:
3rd Parties	<i>Breaches of Information Security Policy that affect or are caused by 3rd parties.</i>	Emails	<i>Receiving information from 3rd parties not intended for our school</i>
		Loss of Information	<i>Our suppliers loses information from our school, or sends information of our school to an incorrect recipient</i>
Breach of Policy	<i>Breaches of Information Security Policy that are not reflected in one of the other options.</i>	Email Misuse	<i>Spam emails, abusive messages, improper use of mailing lists.</i>
		Internet Misuse	<i>Accessing sites in business time, inappropriate sites, use of unauthorised online systems</i>
		Misuse of authority	<i>Misuse of position, access or identity for personal gain.</i>
		Personal Device	<i>Adding an unauthorised personal device to the network or storing schools information on a personal device.</i>
		Information Handling	<i>General lack of good information handling</i>
		Insecure Password	<i>Password for system does not match agreed standard creating additional risk</i>
Data Protection	<i>Breaches of Data Protection law including loss, theft or disclosure of personal information.</i>	Disclosure Personal Information	<i>Confirmed disclosure of personal information to non-intended recipient.</i>
		Loss of Personal Information	<i>Loss of personal information with no certainty it has been disclosed.</i>
		Theft of Personal Information	<i>Theft of personal information with no certainty it has been disclosed.</i>
Lost/ Stolen Equipment	<i>Loss or theft of equipment</i>	Lost Equipment	<i>Lost equipment</i>
		Theft of Equipment	<i>Theft of equipment</i>
Network Security	<i>Incidents that affect the Security of the IT Network storing data.</i>	Spam Email	<i>Spam emails received that pose a threat to the Network.</i>
		Systems Failure	<i>Critical System offline.</i>
		Virus Threat (e.g. Ransomware)	<i>Threat of virus to the network</i>
		Folder Permissions	<i>Reset or corruption of folder permissions for folders on the network</i>

		Unauthorised access to the network	<i>Network accessed by individuals with no lawful right of access</i>
Password Sharing	<i>Incidents where a password has been shared or used by another user.</i>	Password Shared	<i>Member of staff has shared password of a system with another member of staff.</i>
		Logged someone in	<i>Member of staff has logged someone into a system under their own username without sharing the password.</i>
Physical Security	<i>Incidents where the physical security of a building or storage space processing data is compromised.</i>	Insecure Building	<i>Building or storage facility discovered to be insecure.</i>
		Public Unauthorised Access	<i>Unauthorised person has been able to access a building or secured area.</i>

Signed: 
 Head Teacher

Dated: 22nd April 2021

Signed: 
 Chair of Trustees

Dated: 22nd April 2021

