HADLEIGH INFANT & NURSERY SCHOOL

Security Incident Policy

2021-2023

Version	**4**
Document authors	**Sam Proctor**
Other contributors	**IGS**
Policy produced (date)	**September 2022**
Policy approved by	**SIRO / IC / IGG**
Policy approved (date)	**September 2022**
Policy to be reviewed (date)	**January 2023**
Other related policies	**Data Protection Policy** **Data Handling Security Policy** **Acceptable Personal Use Policy** **Statutory Request Policy** **Privacy Notice** **Complaints Policy** **Procedures for Reporting and Handling Security Incidents Policy**

Version History Log for this document

Version	Date Published	Details of key changes from previous version
4	September 2022	Changed references to Mr. S. Proctor to Mrs. D. Glanville - New Head Teacher. No changes made to main body of text.
3	January 2021	Change to most investigations will be overseen by SIRO and not DPO. Actions to support an investigation have changed. SIRO must support with the investigation of major and critical incidents and findings must be referred to the Data Protection Officer.
2	April 2019	Data Protection Act 1998 changed to Data Protection Act 2018
1	April 2018	New policy was created - superseded all previous versions.

Roles within the school

Data Protection Officer (DPO) - Ms. L. Almond

Senior Information Risk Owner (SIRO) - Mrs. D. Glanville

Information Champion (IC) - Mrs. A. Cain

Information Governance Governor - Mr. I. Holroyd

What is a Security incident?

A security incident is a confirmed breach, potential breach or 'near-miss' breach of one of the school's information policies. ***Please refer to Appendix A for examples of Security Incidents.***

What I must do	Why I must do it	How I will do it
If you discover a security incident, you must immediately report it.	Capturing security incidents allows us to respond effectively when something has gone wrong. Capturing all types of security incidents allows us to understand where our weaknesses are, how well our policies are working and what we should change about our policies to make them more effective.	Please notify the school's SIRO or IC. No action will be taken against any member of staff who reports a security incident about another member of staff in good faith. Identification of a reporting party who requests anonymity shall be protected as far as is feasible.
When reporting the incident, you must provide as much information as possible	To help us quickly assess the severity of the incident and to speed up the investigation.	Include full details of the incident such as dates, names and any remedial action that has been taken.
The Investigating Officer must complete investigations and complete an outcome report (see Procedures for Reporting or Handling a Security Incident).	Carry out an effective process appropriate to the severity of the incident.	Where appropriate, undertake the following: A. Identify expected outcomes, stakeholders and any policies breached. B. Speak to staff involved. C. Record evidence and keep an audit trail of events and evidence supporting decisions taken D. Get expert help E. Escalate F. Inform data subjects (service users, staff) where appropriate G. Identify and manage risks of the incident H. Commence disciplinary action, or record why not

		I. Develop and implement a communications plan where appropriate J. Put in place controls to prevent recurrence K. Complete the Incident Outcome Report
All staff must support investigations into incidents as required.	Carry out an effective process appropriate to the severity of the incident.	Where appropriate, undertake the following: A. Work with the SIRO to investigate major security incidents. B. Assess the outcome to ensure the appropriate action has been taken. C. Provide knowledge and advice, and carry out any recommended actions for major or critical incidents, where required.
Maintain a full record of each incident from reporting to closure.	Ensure the process is followed to completion.	Undertake the following: A. Classify the Security Incident B. Verify the details and oversee the investigation C. Work with SIRO to investigate major security incidents. D. Advise, support and intervene as appropriate E. Review Incident Outcome Reports and close
SIRO must support the investigation of major and critical incidents.	Ensure that there is appropriate resource, expertise and independent scrutiny of processes for higher impact incidents.	For major and critical incidents: A. Undertake the investigation (critical only) B. Work with DPO (major only)

		C. Assess if it is necessary for the security incident to be reported to the ICO. D. Complete an outcome report and recommend remedial actions.
Comply with the timescales and escalation process outlined in our Procedures for Reporting or Handling a Security Incident.	Ensure that all incidents are handled in a timely manner.	Follow the process outlined in the ECC Procedures for Reporting or Handling a Security Incident.
Major and critical incidents must be referred to the Data Protection Officer.	Ensure that serious incidents are reviewed against the criteria for reporting to the regulator.	Use contact details the school hold for the DPO. This contact can also be made via IGS.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Mrs. D. Glanville(Head Teacher - SIRO - head@hadleigh-inf.essex.sch.uk)

Breach Statement

Breaches of Information Policies 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.

Contacts

If you have any enquires in relation to this policy, please contact Mrs. D. Glanville(the school's Head Teacher) on 01702557979 or head@hadleigh-inf.essex.sch.uk . The Head Teacher will also act as the contact point for any subject access requests.

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

References

- Data Protection Act 2018

APPENDIX A

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	*Breaches of Information Security Policy that affect or are caused by 3rd parties.*	Secure email	*Issue with GCSx Connection*
		VPN Misuse	*Misuse of Support VPN*
		Loss of Personal Information	*3rd party loss of personal info*
		Loss of Business Information	*3rd party loss of business info*
		Password Sharing	*3rd parties sharing passwords*
Breach of Policy	*Breaches of Information Security Policy that are not reflected in one of the other options.*	Email Misuse	*Spam emails, abusive messages, improper use of mailing lists.*
		Internet Misuse	*Accessing sites in business time, inappropriate sites, use of un-authorised online systems*
		Misuse of authority	*Misuse of position, access or identity for personal gain.*
		Personal Device	*Adding an unauthorised personal device to the network or storing ECC information on a personal device.*
		Information Handling	*General lack of good information handling*
		Insecure Password	*Password for system does not match agreed standard.*
		Staff Tailgating	*Member of staff has tailgated in a building processing data*
		GCSx	*Member of staff has abused the use of their GCSx account*
Data Protection	*Breaches of Data Protection law including loss, theft or disclosure of personal information.*	Disclosure Personal Information	*Confirmed disclosure of personal information to non-intended recipient*
		Loss of Personal Information	*Loss of personal information with no certainty it has been disclosed.*
		Theft of Personal Information	*Theft of personal information with no certainty it has been disclosed.*

Information Complaint	*Complaints received from either the ICO or the public in relation to Information Handling Legislation.*	ICO DP Complaint	*Complaint from the ICO relating to non-compliance with the DP Act 1998*
		ICO FOI Complaint	*Complaint from the ICO relating to non-compliance with the FOI Act 2000.*
		Public FOI Complaint	*Complaint from public relating to non-compliance with the FOI Act 2000.*
		Public DP Complaint	*Complaint from the Public relating to non-compliance with Data Protection law (DPA 1998 & GDPR 2016)*
Lost/ Stolen Equipment	*Loss or theft of equipment (no data stored).*	Lost Equipment	*Lost equipment (no personal data stored).*
		Theft of Equipment	*Theft of equipment (no personal data stored).*
Network Security	*Incidents that affect the Security of the IT Network storing data.*	Spam Email	*Spam emails received that pose a threat to the Network.*
		Mailbox Size	*Large mailbox size or large mailbox size increase within 24 hours.*
		Systems Failure	*Critical System offline.*
		Virus Threat	*Threat of virus to the network*
		Folder Permissions	*Reset or corruption of folder permissions for folders on the network*
		Encryption – Laptop	*Laptop discovered with no Encryption Software installed.*
		Encryption – Desktop	*Desktop discovered with no Encryption Software installed.*
Password Sharing	*Incidents where a password has been shared or used by another user.*	Password Demanded	*Employee has demanded password of a system from another member of staff.*
		Password Shared	*Member of staff has shared password of a system with another member of staff.*
		Logged someone in	*Member of staff has logged someone into a system under their own username without sharing the password*
Physical Security	*Incidents where*	Insecure Building	*Building or storage facility discovered to be insecure.*

	the physical security of a building or storage space processing	Public Unauthorised Access	*Unauthorised person has been able to access a building or secured area.*
Lost/ Stolen Business Information	*Incidents where sensitive information has been lost, stolen or disclosed.*	Disclosure Business Information	*Disclosure of Sensitive Business information*
		Loss Business Information	*Loss of Sensitive Business information with no confirmed disclosure.*
		Theft Business Information	*Theft of Sensitive Business information with no confirmed disclosure.*

APPENDIX B

Security Incident Discovery Referral From			
1. Date of Incident			
2. Name of Team(s) involved			
3. Name of Individual(s) involved		☐ **Not applicable**	☐ **Not known**
4. Details of the Security Incident			
5. What information has actually been lost/ breached?			
6. Name of SIRO or Information Champion this form has been handed to.			
7. Date given to SIRO or Information Champion			
Signed			