MANOR LEAS INFANT SCHOOL

Security Incidents, Information Security & Information Handling Policy

Document Control

Date	Feb 26
Review Date	Feb 27
Policy Number	73
Version Number	V3.0
Author	Data Protection Officer
Approved by	FGB Committee

Contents+

Introduction

Manor Leas Infant 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

The aim of this policy is to ensure security incidents relating to school information and Information Communications Technology (ICT) are managed effectively and consistently.

It supports the schools Information Security Policy.

Scope

The policy applies to:

- School information which is 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 DPO, Heather Brunsden.
- Immediately report all security incidents to DPO, Heather Brunsden.
- Complete the schools security incident reporting form which is at **Annex A** to this policy and send it to DPO, Heather Brunsden.

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.

Information Security

Information Security Responsibilities

The following information security responsibilities are in place to help the school achieve its information security objectives:

- **Governing Body -** The Governing Body has overall responsibility for ensuring the school has appropriate security in place to protect information and ICT and for ensuring compliance with this policy. They also have overall responsibility for information risk management.
- **Head Teacher -** The Head Teacher has day to day responsibility for ensuring individuals are aware of, and apply, this policy. The Head Teacher is also responsible for ensuring that security controls are appropriate and effective.
- **Senior Leadership Team** – The Senior Leadership Team have responsibility for supporting the Head Teacher and Governing Body by ensuring individuals are aware of, and apply, this policy.

- **Individuals** – Every individual has a responsibility to meet the requirements of this policy. This includes complying with individual policy requirements and undertaking training relevant to their role.

Training and Awareness

The school acknowledges that training and awareness plays an important part in creating a culture which takes security seriously. Therefore, the school shall ensure that:

- Staff and Governors undergo information security and data protection training on an annual basis.
- An awareness of security is maintained through regular communications.
- Staff will be encouraged to report security weaknesses.

Information Risk Management

The school shall ensure information risk management forms part of its overall governance.

We will ensure that information risk will be assessed to understand the likelihood of an event happening and the impact of an event should it happen and act accordingly.

Identified information risks will be monitored and reviewed.

Supporting Policies

The school shall produce supporting policies and guidance designed to support individuals in understanding their responsibilities.

Supporting documents include:

- ICT Acceptable Use Policy
- Data Protection Policy
- Data Retention Guidelines

Sensitive Information

You must ensure that care is taken when processing any school information.

Extra care must be taken when processing particularly sensitive information. Such information includes:

- Personal data and special categories of personal data as defined by data protection legislation.

- Any other information that if subject to unauthorised access or amendment, or made unavailable, would cause a negative impact on the school's reputation, finances, service delivery, or people.

You must consider the nature and context of the information you are working with and exercise professional judgement to ensure that school information is always processed appropriately.

General Principles

All information required to deliver services and conduct business has inherent value and therefore requires an appropriate degree of protection.

The confidentiality, integrity and availability of information must be respected at all times.

All staff processing information must take responsibility for ensuring proportionate and reasonable controls are in place, relative to the sensitivity of the information, and in a manner which reduces the risk to that information.

Information must be processed in line with legal and regulatory requirements including information received from, or exchanged with, external partners.

Staff must not access or attempt to access information unless there is a clear and authorised business need.

Personal data must be processed in accordance with the school's Data Protection Policy which supports its obligations under the current data protection legislation.

All staff processing information must undertake annual data protection training and be aware of their individual responsibilities.

See the ICT Acceptable Use policy for guidance around use of personal devices.

Handling and Storing Information

A clear desk (securing information when not in use) and clear screen (locking your screen when not in use) policy must be adopted.

When information, particularly sensitive information, is not in use it must be stored securely e.g. under lock and key.

Ensure all information is protected to prevent unauthorised access.

Information must only be removed from school premises when necessary and when doing so you must ensure it is protected in line with the requirements of this policy.

Printed material must be collected from printers as soon as possible. Secure printing, which requires you to be physically present at the printer to receive the prints, must be used when the facility is available.

Information stored on portable ICT devices such as laptops and smartphones, or removable media, such as CD's and USB sticks must be encrypted.

Do not store information in an unoccupied vehicle. If it is unavoidable because more secure options are unavailable, then you must only store it out of sight in the locked boot of the vehicle. Information must never be stored in a vehicle overnight.

Exercise discretion when discussing school business in public or by telephone. Similarly, you must avoid being overlooked when working.

Before sending sensitive information ensure it is the minimum necessary to achieve your aim. For example, only share personal data with those who have a defined business need to see it and redact documents to remove unnecessary sensitive information.

When redacting information, you must ensure it is done appropriately to prevent accidental disclosure of data. You must also carry out quality assurance checks before releasing the document to ensure redaction is successful.

Transmitting/sending Information

You must take care when transmitting/sending information to others.

By post/courier, you should consider using a 'signed for service' when sending individual mail items containing particularly sensitive information. Your decision should be informed by the additional cost of such a service versus the additional
security benefits i.e. an audit trail. You must use a reputable tracking service for bulk transfer of sensitive information via post to a named individual. Ensure packaging is robust to prevent damage.

By email, you should always double check the recipient to avoid accidental disclosure. Use password protection and encryption where necessary and available. For sensitive information, the receiving party must confirm by email that they are ready for the transfer, that the recipient address is correct and acknowledge that the correct information has been received.

Fax should not be used to send sensitive information.

Information Sharing

Information must only be shared with third parties when there is a legitimate and lawful purpose. All instances of information sharing that involves personal data should be documented.

Before sharing information, particularly sensitive information or personal data, you must:

- Be satisfied that the request has come from a legitimate source
- Take steps to validate the authenticity of the request, where necessary
- Be clear on the purpose for which the information is being requested
- Ensure you are clear on what is being requested
- Where personal data is being requested, ensure there is a lawful basis for sharing

- Be satisfied the request is reasonable and fair, and it is clear why the information is necessary for the purpose
- Take care to avoid oversharing

Information Disclosure

Subject Access Requests are to be directed to the schools Data Protection Officer. These are requests (verbal or in writing) by individuals for copies of personal data we hold about them / their child.

Access to Education Records must be directed to the schools Headteacher. These are written requests by parents for access to their child's Education Record.

Freedom of Information requests are to be directed to the schools Data Protection Officer. These are written requests for any other recorded information held by the school.

Access to CCTV images attracts the same level of control and safeguards as any other personal data.

Destroying Information

You must destroy hard copy information when no longer required. This can be achieved by using a crosscut shredder or by using a confidential waste service.

You must always control access to information until it is securely destroyed. Please see the following link for further information: https://www.gov.uk/government/publications/retention-schedule-for-data-processed-by-dfe/dfe-retention-schedule

Hard copy information is not to be placed in open waste bins or waste skips.

Digital information must be securely deleted from hardware/media when no longer required. Specialist advice can be sought from the school's IT service.

Security Incidents

All security incidents involving information must be reported in accordance with the Security Incident Policy.

Further Information

For further information within the school please contact:

Heather Brunsden
Senior Administrator/Bursar
heather.brunsden@manorleasinfant.org

01522 681810

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

Review

This policy shall be reviewed annually by the Headteacher and a trustee and will be presented to the trustee board.

Annex A – Personal Data Breach Report Form

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)	☐	☐	☐	☐
	Click or tap here to enter text.				
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 heather.brunsden@manorleasinfant.org