Winchelsea

All Individuals Matter

WINCHELSEA PRIMARY SCHOOL
RUSKINGTON

SECURITY INCIDENT POLICY

Introduction

Winchelsea Primary 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 Communication Technology (ICT) are managed effectively and consistently.

It supports the school's 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 PCs; 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 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.

A security incident can impact information in a number of ways:

- Confidentiality – A negative impact on the aim to restrict access to information and/or ICT to those who are authorised to access it.
- Integrity – A negative impact on the aim to maintain the consistency, accuracy and trustworthiness of information and ICT.
- Availability – A negative impact on the aim to ensure information and ICT is available to those who need it, when they need it.

Examples of security incidents include:

- The loss or theft of information;
- Unauthorised disclosure of, or access to, information;
- Loss or theft of ICT;
- Physical security breaches;
- Malicious, intentional, or accidental breach of security policies;
- Insecure disposal of information or ICT;
- Malicious software (malware) infection;
- Web site defacement;

- Social engineering e.g. a fraudulent attempt to gain access to information or ICT.

General Principles

Individuals must report all security incidents accurately and without delay.

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

All reported security incidents will be recorded.

The approach to an incident will consider;

- The type of incident and the nature of any information/ICT involved;
- The impact or potential impact on the school, its staff, parents, children and partners;
- The level of personal data involved;
- The source of the incident.

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

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 Business Manager.
- Immediately report all security incidents to the School Business Manager.
- Complete the schools security incident reporting form which is at **Annex A** to this policy and send it to Mr Steven Guilliatt.

Personal Data Breaches

A personal data breach means a security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, *personal* data.

Personal data breaches attract a number of reporting obligations set out in data protection legislation. All personal data breaches must be recorded on the record of personal data breaches.

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 – Mr Steven Guilliatt.

Further Information

For further information regarding security incidents within the school please contact the Head Teacher.

Further advice and information is available from the ICO at www.ico.org.uk.

Signed: _____ Dated: _____
Chair of Governors

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 Mr Steven Guilliatt – steven.guilliatt@winchelsea.lincs.sch.uk.