Our vision

Challenging expectations and sharing success

Waverley School

Data Protection and Security Incident Reporting Procedure
November 2018

CONTENTS

To be read in conjunction with:

-Whistleblowing Policy
-Retention Policy

1 Definitions

Information Asset	Any information whether paper or electronic held by the school. Examples; a list of pupils on paper, a memory stick.
Security Incident	Any loss, loss of control, disclosure or damage to an information Asset; a compromise of any information asset's confidentiality, availability or integrity
Near Miss	Any incident which **could** have led to a security incident, but was avoided.
PII	Personally identifiable information. Data relating to an identifiable living individual.
DPO	Data Protection Officer; a role defined in the legislation as involved in this process.

2 Purpose

1.1 Any security incident, however caused, could have potentially devastating consequences for pupils, the school or partner organisations and may result in financial loss and legal action.

1.2 The purpose of this document is to define the policies and procedures that will be applied in response to where there has been a security incident or near miss.

1.3 This policy provides direction and support for the implementation of information security and is designed to help school employees carry out the business of the school in a secure manner. By complying with this policy, the risks facing the school are minimised.

1.4 The Data Protection Act 2018 and EU679/2016 General Data Protection Regulation create requirements for incident reporting where PII is involved.

3 Scope

2.1 The school has a responsibility to monitor all incidents that occur within the organisation that may breach security and/or confidentiality of information. All security incidents and near misses need to be identified, reported, investigated and monitored. It is only by adopting this approach that the school can ensure that incidents of a particular nature do not recur, or can be avoided.

3 Introduction

3.1 This procedure applies to:

- The school's workforce
- All Managed Service Providers and organisations that provide a service to the school
- Third party organisations who require access to the school's information systems and facilities should also be aware of the contents of this policy.

The policy is not designed to be obstructive. If you believe that any element of this policy hinders or prevents you from carrying out your duties, please contact the DPO to discuss.

4 Types of Information Security Incidents

4.1 An information security incident is defined as above.

4.2 Examples of these types of incident include, but are not limited to:

- damage to or theft/loss of information (either manual or electronic)
- damage to or theft/loss of IT equipment
- the finding of confidential information/records in a public area
- poor disposal of confidential waste
- unauthorised access to information
- transfer of information to the wrong person (by email, fax, post, or phone)
- receiving of information (such as by email or fax) meant for someone else
- sharing of network IDs and passwords.
- Information being placed on services outside the EU (e.g. web services run from the USA), or services that have not been reviewed and agreed as within the legislation by the DPO
- the disclosure of confidential information to any unauthorised individual

4.3 Every incident must be taken seriously and reported according to the process identified in this document. If there is any doubt about what constitutes a security incident, staff should contact the ICT Security Analyst or the Corporate Systems Assurance Manager or the Departmental Data Coordinator.

5 Staff Training and Awareness

5.1 **All school workforce** have a responsibility to ensure that they and the staff they manage understanding of the requirements of the legislation so that they are able to comply with the requirements.

5.2 Contractors and agents working on behalf of the School should have reference to this procedure in their contracts.

5.1 School workforce must be made aware that if they discover something that could be considered as a security incident, suspected incident or near miss it must be reported immediately to their line manager and an information loss/breach of security incident reporting form completed by the person who makes the discovery.

5.2 If the member of staff prefers to remain anonymous, a name need not be supplied. An individual is not usually entitled to know what is recorded about another individual without their consent.

5.3 This may involve staff reporting observed or suspected incidents or actions of others where security is threatened. See the School's Whistle Blowing Policy.

6 Reporting of Incidents / Near Misses

6.1 The person reporting an incident or near miss must fill in the Security and Data Protection Incident reporting form as soon as the incident/near miss is recognised. It is more important that the incident is reported than all data on the form be completed.

6.2 The completed (or partially completed) Security Incident/Risk Reporting Form should be sent to:

- the head teacher and
- the Data Protection Officer

6.3 The DPO will inform Information Governance Board members and/or the Caldicott Guardian if appropriate).

6.4 The head teacher will inform the governing body.

6.5 The DPO will assist the school and the head teacher in completing the incident form, assessing the impact of the incident and reporting to the ICO and data subjects as required.

7 Recording of Incidents

7.1 Details of incidents will be recorded in the DPO monitoring spreadsheet for monitoring and reporting purposes.

7.2 The Information Security Incident/Risk Reporting Form, with any associated documents, will be retained in accordance with the School's Retention Policy

8 Management Reporting

8.1 The DPO will review and assess all reported incidents and provide advice and guidance to the school.

8.2 Security incidents will be reported to the Security Working Group and the Information Governance Board for further action as appropriate (if there are council consequences). Schools are recommended to include this in their governor reports and the DPO will assist in facilitating this.

8.3 All registered incidents will be investigated and re-evaluated after a 6 month period to ensure the type of incident is no longer being reported or the volume of those incidents has reduced.

8.4 If there is no reduction in the volume of each type of incident the Information Governance Board will be alerted by the ICT Security Analyst and appropriate action taken. This could be further training and awareness for staff or an improvement to existing security and/or confidentiality policies and procedures.