Waverley School

Cyber and Information Security Policy

November 2018

Contents

Required/recommended to adhere to in conjunction with this policy:

- Data Protection Act 2018 (included the Applied General Data Protection Regulation EU679/2016)
- Freedom of Information Act 2000
- ISO 15489 International Standard for Record Management
- ISO 27001
- E-Government Interoperability and Metadata Frameworks
- UK Gov Minimum Cybersecurity standards
- PCI-DSS requirements (if card data is used)
- PSN Code of Connection requirements
- Access to Health Record Act 1990
- Access to Personal Files Act 1987
- Legal admissibility and Evidential weight of Information stored electronically (British Standard Code of Practice BIP 0008)
- Common Law Duty of Confidence
- Human Rights Act (Article 8)
- Caldicott Principles

1. Purpose

This document provides the overarching governance policy for the protection and security of our school data and information.

The policy aims to define the high-level governance of Cyber Security within the school.

2. Objectives

The main objectives of this policy are:

- To present the management approved requirements, control objectives and principles for Cyber Security.
- To define the structure and roles within our school's Cyber Security structure
- To maintain confidence that our school's Cyber Security governance meets its corporate and ICT risk appetite.
- To maintain confidence that our school's Cyber Security governance meets the requirements of the law including the data protection regulations, the guidance on government use of cloud services and other compliances as required.

3. Scope

This policy applies to all ICT systems, data and information directly or indirectly via third parties in use by our school.

4. Policy Mandate, Approval and Maintenance

This policy is approved by the board of governors.

The policy will be reviewed regularly and at least annually, and in case of any impacting changes (for example, changes to HMG policy, legislation, regulation, industry standards, school ICT environment, etc.), to ensure it remains current, appropriate and applicable.

5. Definitions

Name	Definition
Information Asset	Any item of data kept by the school. For example a pupil record is an information asset.
Record	Generally a synonym for information asset. Some policies require a defined "Record manager".
Cyber Security	Ensuring that electronic records are protected. Basically a synonym for "information security".

6. Policy

6.1 Requirements, Control Objectives and Principles

1. **Risk Appetite.** The school has a defined risk management policy available on the School drive.
2. **Compliance.** Our school is required to comply with law and with certain regulations. This policy mandates compliance with, at a minimum:

    - General Data Protection Regulation / Data Protection Act (GDPR / DPA)
    - UK Minimum Cyber Security Standard

6.2 Roles

1. **Data Owner**. The person responsible for the data and compliance in a particular area or system. Generally this will be the Head Teacher. The Data Owner is recorded in the GDPR Workbook for each information asset area.
2. **Senior Information Risk Owner (SIRO)**. The risk decision maker for the school. This is the Head Teacher.
3. **Board of Governors Lead for Information Governance**. The Governor with overall responsibility for the oversight of information governance for our school.
4. **Data Protection Officer.** The independent person providing advice to the authority on compliance, dealing with public complaints and acting as interface to the regulator.
5. **School Business Manager.** The person responsible for day-to-day management of school data and ensuring compliance alongside headteacher.
6. **Records Manager.** The owner of records management across the school, responsible for ensuring information assets are preserved and destroyed appropriately. This is the Schools Business Manager inline with the headteacher.

6.3 Boards

1. **Senior Leadership Team.** The forum working on behalf of and reporting to the SIRO that is empowered to:
    - Review and agree day-to-day operational risk decisions
    - Take decisions regarding data usage within the school, in consultation with the Data Protection Officer

- Create reports for the board of governors regarding cyber risk and information usage within the school.
- Assure the Board of Governors that risks are being managed effectively in accordance with their risk appetite and policies and controls are adequate and enforced;
-

2. **Board of Governors**
    - set the strategic direction for and approve applicable information; governance, privacy (including surveillance) and security policies;
    - receive reports on the information governance, privacy and security status of the organisation, including internal audit, and ensure effective investigation of and organisational learning from complaints, incidents and near-misses;
    - ensure compliance with required standards and legislation, overseeing training and testing and making recommendations to EMT as appropriate;
    - oversee registration with the ICO
    - ensure effective records and data management across the organization;

7. Applicable Standards

There are a number of standards applicable to Cybersecurity and Information Management that the school is required or recommended to adhere to. These are:

- Data Protection Act 2018 (included the Applied General Data Protection Regulation EU679/2016)
- Freedom of Information Act 2000
- ISO 15489 International Standard for Record Management
- ISO 27001
- E-Government Interoperability and Metadata Frameworks
- UK Gov Minimum Cybersecurity standards
- PCI-DSS requirements (if card data is used)
- PSN Code of Connection requirements
- Access to Health Record Act 1990
- Access to Personal Files Act 1987
- Legal admissibility and Evidential weight of Information stored electronically (British Standard Code of Practice BIP 0008)
- Common Law Duty of Confidence
- Human Rights Act (Article 8)
- Caldicott Principles

8. Policy Exceptions and Violations

Any employee, contractor, partner, service provider or other entity who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written formal complaint or Exception Request, via his or her manager or other manager to the School's SIRO. Complaints may be dealt with by managers and the HR Department. All Exception Requests must first be approved by the SIRO.

Any violation of this policy may result in disciplinary action, up to and including termination of employment. The School reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. The School does not consider conduct in violation of this policy to be within an employee's or partner's course and scope of employment, or the direct consequence of the discharge of the employee's or partner's duties. Accordingly, to the extent permitted by law, The School reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.