RUSSET HOUSE SCHOOL

Cyber and Information Security Policy

Author	**DPO**	Classification	**OFFICIAL**	Date of First Issue	**07/08/2018**
Owner	**Data Protection Officer**	Issue Status	**FINAL**	Date of Latest Re-Issue	**08/06/2022**
Version	**1.3**	Page	**1 of 6**	Date approved by Govenors	
Reviewer	**Sharlene Morris (DPO)**			Date of next review	**28/10/2024**

May 2026

Contents

1. Purpose 3
2. Objectives 3
3. Scope 3
4. Policy Mandate, Approval and Maintenance 3
5. Definitions 3
6. Policy 4
   6.1 Requirements, Control Objectives and Principles 4
   6.2 Roles ....
   6.3 Boards 4
7. Applicable Standards 5
8. Policy Exceptions and Violations 5

This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

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 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 school policies, 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's governors have agreed this policy and accepted the following statements on risk appetite:
   - The school wishes to use state of the art technologies and will accept a level of risk created by this.
   - The school will risk assess each information assets use as required by the data protection legislation and record actions it has taken.
   - The school will work to minimise all risks to personal data to a level commensurate with the normal industry practice
   - The Head Teacher is responsible for managing information risk

2. **Compliance.** Our school is required to comply with law and with certain regulations. This policy mandates compliance with, at a minimum:

   - UK General Data Protection Regulation / Data Protection Act (UK GDPR / DPA)
   - DfE's **Cyber Security Standard**

6.2 **Roles** All roles and responsibilities can be delegated.

1. **Data Owner**. The person responsible for the data and compliance in a particular area or system. Generally, this will be the Head Teacher.
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.
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.

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

- 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 SLT as appropriate.
    - Oversee registration with the ICO.
    - Ensure effective records and data management across the organisation.

7. Applicable Laws and 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:

- DfE's **Cyber Security Standard**
- Data Usage and Access Act 2025
- Data Protection Act 2018
- UK General Data Protection Regulation
- 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 BS10008)
- 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 the School Business Manager.

Complaints may be dealt with by the School Business Manager, the HR. 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 governing body or law enforcement authority of any serious non-compliance or 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.