HALES VALLEY TRUST

Information & Cyber Security Policy for Schools

Policy Tracker – Responsibility for monitoring this policy: COO (Reviewed annually – date of next review September 2021)			
Date of review	**Reviewed By:**	**Role**	**Date Approved by the Governing Board/committee**
December 2020	Racheal Jones	COO	N/A
December 2020	Rachel Evans	Operations Manager	N/A

1. Policy Statement

Hales Valley Trust will ensure the protection of all information assets within the custody of the School.

High standards of confidentiality, quality and availability of information will be maintained at all times.

Hales Valley Trust will demonstrate support for, and commitment to, information and cyber security through the issue and maintenance of an information and cyber security policy within the school including the supporting guidance documents which are listed below.

2. Purpose

Information is a major asset that the school has a responsibility and requirement to protect. The secure running of the school is dependent on information being held safely and securely.

Information used by the school exists in many forms and this policy includes the protection of information stored electronically, transmitted across networks and printed or written on paper. It also includes any information assets in Cyberspace (The Cloud). UK Cyber Security Strategy 2011 defined Cyberspace as:

"Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services".

Protecting personal information is a legal requirement under Data Protection Law.

The school must ensure that it can provide appropriate assurances to its pupils, parents and staff about the way that it looks after information ensuring that their privacy is protected and their personal information is handled professionally.

Protecting information assets is not simply limited to covering the information (electronic data or paper records) that the school maintains. It also addresses who has access to that information, the processes they follow and the physical computer equipment used to access them.

This Information Security Policy and associated guidance documents, as listed below, address all of these areas to ensure that high confidentiality, quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of information assets.

3. Scope

This Information Security Policy and associated guidance documents, as listed below, apply to all systems, people and school processes that make up the school's information systems. This includes all Governors, school staff and agents of the school who have access to Information Systems or information used for school purposes.

4. Definition

This policy should be applied whenever school information systems or information is used.

Information can take many forms and includes, but is not limited to, the following:

• Hard copy data printed or written on paper.
• Data stored electronically (on site, on a network or in the cloud).
• Communications sent by post / courier or using electronic means.
• Stored tape or video.
• Speech.

5. Risks

The school recognises that there are risks associated with users accessing and handling information in order to conduct official school business.

The school is committed to maintaining and improving information security and minimising its exposure to risks. It is the policy of the school to use all reasonable, practical and cost effective measures to ensure that:

- Information will be protected against unauthorised access and disclosure.
- The confidentiality of information will be assured.
- The integrity and quality of information will be maintained.
- Authorised staff, when required, will have access to relevant school systems and information.
- Business continuity and disaster recovery plans for all critical activities will be produced, tested and maintained.
- Access to information and information processing facilities by third parties will be strictly controlled with detailed responsibilities written into contract/documented agreements.
- All breaches of information and cyber security, actual and suspected, will be reported and investigated. Corrective action will be taken.
- Information security training will be available to all staff.
- Annual review of Information and Cyber Security Policy and associated guidance documents, as listed below, will be carried out.
- This policy will be reviewed when significant changes, affecting the school are introduced.
- An Information Security framework of policies and guidance will be developed and implemented consistent with this policy.

- The school's Information and Cyber Security arrangements will be subject to review by the Senior Information Risk Owner (SIRO) supported by the school's Data Protection Officer.

Non-compliance with this policy could have a significant effect on the efficient operation of the school and may result in financial loss and embarrassment.

6. Roles and Responsibilities

It is the responsibility of each member of staff to adhere to this policy, standards and procedures. It is the school's responsibility to ensure the security of their information, ICT assets and data. **All** members of the school community have a role to play in information security. Refer to Appendix 1 for information on the role of the Senior Information Risk Owner (SIRO), Data Protection Officer (DPO) and Information Asset Owners (IAO).

7. Supporting Guidance Documents

The following guidance documents are directly relevant to this policy.

- Data Protection Policy
- E-Safety Policy for Schools
- Homeworking Guidance
- Staff Guardianship Form
- Bring your own device to work
- Information Asset Registers
- Security Incident Reporting Guidance
- Policy Governing the operation of CCTV

Appendix 1

1. Roles and Responsibilities

Role of the Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff within the school who is familiar with information risks and the school's response. Typically, the SIRO should be the Headteacher or a member of the Senior Leadership Team and have the following responsibilities:

- Own and maintain the Information Security Policy.
- Establish standards, procedures and provide advice on their implementation.
- Act as an advocate for information risk management.
- Appoint the Information Asset Owners (IAOs).

Additionally, the SIRO will be responsible for ensuring that:

Staff receive appropriate training and guidance to promote the proper use of information and ICT systems. Staff will also be given adequate information on the policies, procedures and facilities to help safeguard the school's information. A record of the training provided to each individual member of staff will be maintained.

Staff are made aware of the value and importance of school information particularly information of a confidential or sensitive nature, and their personal responsibilities for information security.

The associated guidance relating to information security and the use of particular facilities and techniques to protect systems and information, will be disseminated to staff.

The practical aspects of ICT protection are performed, such as maintaining the integrity of the data, producing the requisite back-up copies of data and protecting the physical access to systems and data.

There are appropriate controls over access to ICT equipment and systems and their use including defining and recording the requisite level of protection.

They are the official point of contact for ICT or information security issues and as such have responsibility for notifying the Senior Leadership Team, Data Protection Officer and Chair of Governors of any suspected or actual breach occurring within the school.

The school's Senior Information Risk Officer (SIRO) is the Chief Operations Officer (COO).

Role of the Data Protection Officer (DPO)

Article 37 of the General Data Protection Regulation (UK GDPR) mandates that schools and academies have a Data Protection Officer (DPO) in place.

The role of the DPO within school is to:

- Advise the school, their data processors and their employees of their responsibilities.
- Monitoring school's compliance with UK GDPR and other data protection legislation and internal policies.
- Advising on data protection impact assessments.
- Monitoring performance.
- Identifying safeguards to apply to mitigate any risks identified.
- Maintain a record of processing activities.
- Maintain records and evidence of the school's compliance with the UK GDPR.
- Conduct audits to ensure compliance and address potential issues (including an annual benchmark audit).

The DPO will also be the contact point for the Information Commissioner's Office (ICO).

The schools Data Protection Officer is James Gray at Information Governance, Dudley.

Role of the Information Asset Owner (IAO)

Once the School has identified its information assets, including personal information and data relating to pupils and staff, for example, assessment records, medical information and special educational needs data, schools should identify an Information Asset Owner (IAO) for each asset or group of assets as appropriate.

The role of an IAO is to understand:

- What information is held and for what purposes.
- How information will be amended or added to over time.
- Who has access to the data and why.
- How information is retained and disposed of.

Typically, there may be several IAOs within a school, for example, School Admin teams, IT Manager.

The IAO is responsible for managing and addressing risks to the information and ensuring that information handling both complies with legal requirements and is used to fully support the delivery of education.

Important information assets will include, but are not limited to, the following:

- Filing cabinets and stores containing paper records e.g. archives.
- Computer databases.
- Data files and folders.

On the introduction of this policy Information Asset Owners may need to conduct a thorough information risk assessment to identify any necessary operational or technological changes that may be required within the school.