Sutton School and Specialist College Policy

For

Information and Security Policy

Date of first issue: 3rd May 2018

Dates of Updates:

Most recently approved by governors on: TBC

To be next reviewed on:

Information & Cyber Security Policy for Schools

1. Policy Statement

Sutton School & Specialist College 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.

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 the Data Protection Act 1998.

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 addresses 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 applies 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.

This policy aims to mitigate the following risks:

• The non-reporting of Information Security incidents
• The inadequate management of records
• The inadequate destruction of data
• The unauthorised user access to information, Information Systems and facilities

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) and Information Asset Owners (IAO).

7. Guidance Documents

The following guidance documents are directly relevant to this policy.

- Data Protection Policy
- E-Safety Policy for Schools (DGfL)
- Technical Controls Policy (DGfL)
- Homeworking Guidance
- Staff Guardianship Form (DGfL)
- Bring your own device to Work (DGfL)
- Protective Marking
- 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 and Chair of Governors of any suspected or actual breach occurring within the school.

The school's Senior Information Risk Officer (SIRO) is Mr D Charles (Headteacher)

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, Business Manager, ICT 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.