# Information, IT and Cyber Security Policy

February 2023

## 1. Policy Statement

Holmer Green Senior School will ensure the protection of all information assets within its custody.

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

## 2. Purpose

Information is a major asset that the Academy 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 Academy 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 maintain. It also addresses who has access to that information, the processes they follow and the physical computer equipment used to access them.

This Information, IT and Cyber 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 and exists to ensure that all staff and students follow certain basic rules with regard to internet use and use of IT in general. Its aim is to prevent students or staff coming to harm as a result of others accessing intolerant, extremist or hateful web sites. Also, it is here to protect students and staff from cyber bullying.

## 3. Scope

This Information, IT and Cyber Security Policy applies to all systems, people and school processes that make up the Academy'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. 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

## 4. Risks

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

The Academy is committed to maintaining and improving information security and minimising its exposure to risks. It is the Policy of the Academy 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 and logged (including access to all computer rooms), with detailed responsibilities written into contract/documented agreements
- All breaches of information, IT and cyber security, actual and suspected, will be reported and investigated. Corrective action will be taken.
- Information security training will be mandatory for all staff
- Staff cyber security training each term to include start of term email remember to staff to comply with RPA requirements
- Annual review of Information, IT and Cyber Security Policy will be carried out
- This policy will be reviewed annually
- The Academy's Information, IT and Cyber Security arrangements will be subject to review by the Senior Information Risk Owner (SIRO) supported by the Academy's Data Protection Officer

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

## 5. Use of the internet including all Social Media sites

HGSS will provide Internet access to teachers and students for the primary purpose of study, legitimate research, email access and general internet access. The availability and variety of information on the Internet has meant that it can be used to obtain material reasonably considered to be offensive. The use of the Internet to access and/or distribute any kind of offensive material, or material that is not work or study related, leaves an individual (staff and students) liable to disciplinary action which could lead to dismissal (staff) or suspension (students). Staff are expected to follow all guidance issued to protect the academy's IT systems from cyber-attacks from external sources.

**HGSS Internet and IT provision may not be used for:**

- transmitting, retrieving or storing any communications of a discriminatory or harassing nature
- transmitting, retrieving or storing any communications which are derogatory to any individual or group
- obtaining material that would cause offence on the grounds of race, colour, religion, political beliefs, ethnic origin, sexual orientation, gender, age, disability, nationality, marital status,
- engaging in ANY form of cyber bullying
- searching for obscene, offensive, sexually explicit or pornographic material
- obtaining any material for the purpose of harassment of another person
- establishing communications which are defamatory or threatening
- obtaining material that is unlawful or that infringes on another person's legal rights (e.g illegal downloads)
- **conducting internet searches and looking at websites which can in any way be regarded as extremist, intolerant of other's faiths and beliefs, or that challenge the rule of law and the right to individual liberty**

### Monitoring Use of Computer Systems

HGSS has the right to and does monitor electronic information created and/or communicated by students or staff using HGSS computer systems and networks, including e-mail messages and usage of the Internet

## 6. E-mail

The use of the E-mail system is encouraged as its appropriate use facilitates efficiency. Used correctly it is a facility that is of assistance to employees. Inappropriate use however causes many problems including distractions, time wasting and legal claims. The procedure sets out the Academy's position on the correct use of the E-mail system.

- Unauthorised or inappropriate use of the E-mail system may result in disciplinary action which could include summary dismissal.
- The E-mail system is available for communication and matters directly concerned with the legitimate business of HGSS. Employees using the E-mail system should give particular attention to the following points:-
  1. all comply with Academy communication standards;
  2. E-mail messages and copies should only be sent to those for whom they are particularly relevant;
  3. E-mail should not be used as a substitute for face-to-face communication or telephone contact. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding;
  4. if E-mail is confidential the user must ensure that the necessary steps are taken to protect confidentiality.
  5. offers or contracts transmitted by E-mail are as legally binding on HGSS as those sent on paper.
- HGSS will not tolerate the use of the E-mail system for unofficial or inappropriate purposes, including:-
  1. any messages that could constitute bullying, harassment or other detriment;
  2. personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);
  3. on-line gambling;
  4. accessing or transmitting pornography

## 7. Roles and Responsibilities

It is the responsibility of each member of staff to adhere to this Policy, standards and procedures and in particular to take very seriously the threat from phishing scams and to never give away their personal login details/passwords. It is the Academy’s responsibility to ensure the security of their information, IT assets and data. **All** members of the Academy community have a role to play in information security.

### 7.1 Role of the Senior Information Risk Owner (SIRO)

The SIRO is a senior member of staff within the Academy who is familiar with information risks and the school’s response. The SIRO for HGSS is the Business Manager and they have the following responsibilities:

- own and maintain the Information, IT and Cyber Security Policy
- establish standards, procedures and provide advice on their implementation
- act as an advocate for information risk management

Additionally, the SIRO will be responsible for ensuring that:

- Staff receive appropriate training and guidance to promote the proper use of information and IT 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 practical aspects of IT 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 IT equipment and systems and their use including defining and recording the requisite level of protection.

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

- The SIRO 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

The SIRO may need to conduct a thorough information risk assessment to identify any necessary operational or technological changes that may be required within the Academy.

### 7.2 Role of the Data Protection Officer (DPO)

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

The role of the DPO within the school is to:

- Advise the school, their data processors and their employees of their responsibilities
- Monitoring the schools compliance with UK GDPR and other data protection legislation and internal policies
- Advising on data protection impact assessments
- Monitoring performance

The DPO will for Holmer Green Senior School is Mark Purdom – email: mark@douc.tech
The SIRO and Data Protection Lead for Holmer Green Senior School is Lynda Jackson, Business Manager – email: jacksonl@holmer.org.uk
This Policy should be read in conjunction with the school's GDPR Policy and ICT Acceptable User Policy.

Approved by Governing Body: February 2023

Next Review: February 2024