SPRING HILL HIGH SCHOOL	Cyber Security Policy
Person(s) Responsible:	
Approval:	Governing Body
Headteacher:	Gary Edmunds
Policy Originator:	Chris Delahaye
Date Approved:	September 2020
Date of Review	September 2021
Read in conjunction with:	Data Protection (GDPR) Policy; Privacy Notice; Acceptable Use Policy; Safeguarding Policy

Policy Statement

The purpose of this policy is to outline cybersecurity strategies that prevent unauthorised access to organisational assets such as computers, networks and data. It is intended to be read in conjunction with the Data Protection Policy. This policy relates more specifically to, and outlines Spring Hill High School's (the school's) approach in satisfying, Article 25 of the General Data Protection Regulations (GDPR), data protection by design and default. In short, the technical security measures that are in place in order to assist in the protection of personal information, alongside the 'organisational measures' outlined in the Data Protection Policy. That is, a set of cybersecurity strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. It maintains the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers.

Rationale

1. **Protection of personal and sensitive information**

The GDPR requires organisations to integrate data protection concerns into every aspect of processing activities and is focused on accountability (our ability to demonstrate compliance).

Article 25(1) specifies the requirements for data protection by design:

'Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at

the time of the determination of the means for processing and at the time of the processing itself, implement **appropriate technical and organisational measures**, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.'

It is focused on maintaining the confidentiality, integrity and availability of personal and sensitive information. The aim is to protect, to consistently high standards, all information assets including students', staff's, parents' and carers' and other third parties' records, written or electronic and all other corporate information, from all potentially damaging threats, internal or external, deliberate or accidental, imagined or real.

Until the advent of the internet, cyber was used in the information of words relating to computers, computer networks, or virtual reality. From the Wall Street Journal to Doctor Who cyber has developed into the English language where it is currently associated with the Internet and other developing technologies. Mass cyber attacks are almost always via Internet providers data systems which are hacked and often the data is leaked into the mainstream media outlets. Governments now issue lots of guidance regarding cyber breaches of data protection laws and this policy reflects much of the guidance.

The Information Commissioner has advised schools to be particularly vigilant around information security. It has warned that unauthorised access to personal information would be particularly harmful to pupils, parents and staff; people with a right to seek compensation if the loss of their personal data caused them damage.

Action Fraud, the UK cybercrime and fraud reporting centre warned schools in January to be wary of cybercriminals claiming to be from the 'Department of Education'. This followed a series of incidents in which bogus emails were used to infect school computer systems with malicious software that prevented legitimate users from accessing them.

2. Other risks

While these risks are relevant to any organisation with personal data and computers, schools are particularly exposed to several other risks relating to online safety, including:

- Exposure to sexually explicit, racist, violent and extremist content
- Inappropriate contact from people who may wish to abuse, exploit or bully them
- Students themselves engaging in harmful online behaviour

The Policy

Where information security is cited, it includes cyber security and vice versa.

Information security is primarily about people, but is facilitated by the appropriate use of technology, which is evermore sophisticated and evolving in its nature.

This policy applies to all aspects of information handling, including, but not limited to

- use of school hardware including staff laptops and student desktop computers
- structured record systems – paper and electronic
- information recording and processing systems – paper, electronic, video, photographic and audio recordings
- information transformation systems such as fax, email, portable media, post and telephone

The purpose of the policy is to achieve a consistent approach to the security management of information throughout the school, in order to enable continual business capability and to minimise the likelihood of occurrence and the impact of any information security incident or security breach.

Physical Security Measures

The physical security of information is the responsibility of everyone who is involved in the handling, maintaining, storage, retrieval, including any information which is shared, transmitted electronically or transported by external suppliers e.g. courier services and postal deliveries. Staff at all levels throughout the school must take all necessary precautions to avoid loss, theft, damage or misappropriation of information. The following good practice is in place.

- all staff must carry I.D. badges; individuals not doing so, in non-public areas should be challenged
- visitors must sign in, be met at a reception area and accompanied at all times
- all doors must be properly secured and where used, entry codes must be regularly changed to protect their integrity
- anyone loitering or obviously out of place should be asked their purpose of visit etc and checked accordingly

Digital Security Measures to address risks

The following organisational measures are in place to ensure the safety of our students and other data subjects:

1. **Confidentiality, integrity and availability of information**

G Suite for Education and Schoolpod

- Administrative functions (e.g. sharing permissions, mail redirects, login challenges) are reserved to the G Suite Administrator and Head Teacher's PA. No other individual has access to the administrator login credentials
- Strong passwords and 2-step authentication (text message or email) are required to log in to the school's G Suite
- Administrative settings are in place to limit sharing outside of the organisation, unless with specified persons by administrator, subject to identity checks
- 'Layered access' to files and folders contained in the school's staff shared drive is in place. Access to confidential information is restricted to only individuals that require access, and only for as long as necessary

- Two distinct 'shared drives' are in place, one accessible by staff and another by students, to avoid confidential documents being wrongfully shared with unauthorised persons
- All staff are trained in data protection, secure processing and sharing to an appropriate level in order to carry out their job role
- Upon a member of staff leaving the organisation their user profiles used to access G suite, Gmail and Schoolpod are removed immediately

Staff and Student Computers

- Web (URL) filtering and usage monitoring software is installed on all staff and student computers. The widest level of protection is offered. Blocked content includes sexually explicit or violent material, gambling, malware, phishing
- Auto-lock if system remains idle (minimum timescale)
- IT systems audits are carried out termly to ensure all organisational devices are accounted for and there is no unauthorised access to the network

2. Other risks

- Exposure to sexually explicit, racist, violent and extremist content
    - All staff are trained in PREVENT in order to identify pupils at risk and take appropriate action to respond to concerns
    - The school maintains regular contact with parents and carers and operates transparently with the team around the child with regards the sharing of information relating to the risk of accessing such content
- Inappropriate contact from people who may wish to abuse, exploit or bully them
    - The school's contemporary internet safety curriculum is accessed by all students and reinforced regularly. It includes the following themes:
        A. Cyberbullying
        B. Cyber security threats and measures to mitigate risk
        C. Hackers and Online fraud
        D. Malicious software
        E. Grooming, sexting and image sharing
        F. Physical safety

Staff Responsibilities

Staff must adhere to the following measures to mitigate cyber security risks:

- If staff leaves their workspace they must close the chromebook screen, or use screen lock if using a windows system (*windows button + L*). Screens should be locked when unattended even for short periods, such as toilet breaks
- Staff must use identified encryption software (*egress switch*) when using email communication to transfer personal or special category information (as outlined in Data Protection Policy (GDPR)) of learners, staff or any other person to external agencies and professionals outside of the organisation
- in order to prevent a malware contamination, no external hardware such as USB, Memory or Recording Portable Devices is permitted to be used within the school, without prior approval from the IT Department

- Management of computers and/or networks is controlled via a contractual arrangement with our umbrella organisation (Lindale Homes) IT Department
- Users shall not install software onto any school IT system, for any purpose, unless authorised to do so by the IT Department. Administrator privileges are required in order to install any software
- passwords should never be shared with any other person
- disposal of equipment is allowed only by authorised personnel
- should a legitimate need arise for a non-routine transfer of information, a risk assessment must be undertaken first to determine the most secure transfer process e.g. courier, by hand only, etc
- adequate and appropriate monitoring of information that is held and its use, should be undertaken at least annually, as part of the audit cycle
- records management systems, policies and procedures should be followed at all times, within the information chain
- paper information is particularly vulnerable, for instance, person identifiable, sensitive personal information should be removed or covered when left unattended on desks or work surfaces
- a clear desk routine should be followed, with a final check in place at the end of the working day, which includes paper vulnerability and computer security

Business continuity is assured by continually reviewing our information systems, in particular;

- that information shall be available to properly authorised personnel as and when it is required
- relevant information security awareness and training is regularly available and accessible to staff
- all breaches of information security, actual or suspected are recorded, reported and investigated and mitigating measures put into place to prevent a re-occurrence

Potential or Actual Security Breaches

- all staff within this school are responsible for ensuring that no potential or actual security breaches occur as a result of their actions.
- on receipt of a reported breach, an investigation with a report, in a timescale appropriate to the risks to the business, will be completed by Data Protection Officer
- notifications to any Regulatory body will be part of this process, where necessary

More information about breaches is outlined in the Data Protection Policy

Assessment of Risk

Risk to the business is directly linked to our capacity to remain secure and any such measures must be viewed as a necessary protection against any event occurring. A range of security measures can be deployed to address:

- the **Threat** of something damaging the confidentiality, integrity or availability of information held or systems or manual records
- the **Impact** that such a threat would have

- the l**ikelihood** of such a threat occurring

To mitigate risks, we will work towards a "paperlite" environment.

Information Sharing Guidance

This clarifies information sharing for staff at all levels of the school. Where staff are in any doubt as to whether it is appropriate to share information, advice should be sought from senior leaders or appointed Data Protection Officer.

Information Sharing Principles

- Must have lawful authority
- Must be necessary
- Must be proportionate
- Must need to know
- Must be accountable
- Must ensure the safety and security of the information shared

We are all aware of the intense media interest particularly when things go wrong, so a balanced approach to information sharing is vital in any decision to share. In safeguarding situations particularly, it is important to ask why you wouldn't share. Information that has been provided in confidence is not normally shared or used without consent from the subject and source of such information. In all cases the main legislation which underpins the sharing of information in relation to adults at risk is:

- Common law duty of confidentiality
- Data Protection Act 1998
- General Data Protection Regulations (GDPR 2018)
- Human Rights Act 1998
- Freedom of Information Act 2000
- Crime and Disorder Act 1998
- Care Act 2014

It is a requirement that all staff of this school adhere to the Golden Rules, set out below, for information sharing in all instances of information Exchange between all multi-agency partners external contacts and any request for such information will only be shared when all the Golden Rules are met.

The Golden Rules

- remember that the Data Protection Act is not a barrier to sharing information but provides a framework to ensure that personal information about living persons is shared appropriately
- be open and honest with the person, family or representative from the outset about why, what, how and with whom the information will or could be shared
- seek advice, if you are in any doubt, and where this is outside of the school, remember confidentiality

- share with consent, where appropriate and where possible, respect the wishes of those who do not consent to share confidential information
- you may still share information without consent, if, in your judgement, that lack of consent can be overridden in the public interest. you will need to base such judgements on the facts of the case
- consider safety and well-being: base your information sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions
- adhere to all policies regarding transporting of confidential and sensitive information including staff records

Failure to comply with this policy

If a member of staff knowingly, or recklessly, or otherwise does not act in accordance. may result in additional training (disciplinary action). This may amount to gross misconduct and result in disciplinary procedures, depending upon the level of harm and culpability.

Guidance

- The National Cyber Security Centre (NCSC). www.ncsc.gov.uk
- The National Security Strategy 2016 – 2021 www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
- The Information Commissioner's Office (ICO). https://ico.org.uk/
- HSCIC now NHS Digital www.gov.uk/government/organisations/health-and-social-care-information-centre http://content.digital.nhs.uk/
- Cyber Aware www.cyberaware.gov.uk
- Cyber Essentials (CE) www.cyberessentials.ncsc.gov.uk
- Get Safe Online www.getsafeonline.org
- Action Fraud www.actionfraud.police.uk
- ISO/IEC 27001 – Information Security Standard. www.iso.org/isoiec-27001-information-security.html
- ISO/IEC 27002 - Security techniques - Code of practice for information security controls www.iso.org/standard/54533.html
- ISO/IEC 27005 - Information Security Risk Management www.iso.org/standard/56742.html
- ISO/IEC 22301 – Business Continuity Standard. www.bsigroup.com/en-GB/iso-22301-business-continuity/
- ISO/IEC 22313 - Business Continuity Management Systems — Guidance www.bsigroup.com/en-GB/Cyber-Security/Cyber-security-for-SMEs/Managing-your-IT-and-cyber-security-incidents/Standards-for-managing-IT-security-incidents/
- Strong Password Generator. https://strongpasswordgenerator.com/