SHREWSBURY HOUSE SCHOOL

INFORMATION SECURITY POLICY

Table of Contents

1. Introduction and Overview

a. Scope

This document applies to all the users in the Shrewsbury House School Trust (SHS Trust) which is comprised of Shrewsbury House School, Shrewsbury House Pre- Preparatory School (SHPPS) and The Rowans. It also includes temporary users, visitors with temporary access to services and third-party partners with limited or unlimited access to information used for the daily functioning of the SHS Trust. Compliance with policies in this document is compulsory for all who have access to information at the SHS Trust.

The Information Security Policy applies to all forms of information, including, but not restricted to text, pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned, administered or controlled by the SHS Trust. It includes information which is:

- Spoken face to face, by phone, or by two-way radio
- Written on paper or printed from a computer
- Stored physically in filing cabinets
- Transmitted and stored in the email system (G-Suite)
- Stored and processed via computer, computer networks or mobile devices
- Stored on any type of removable computer media.

b. Purpose

This purpose of the Information Security Policy is:

- To highlight the information security arrangements across the SHS Trust.
- Protect the SHS Trust and users to the maximum extent possible against security risks that could endanger the integrity, privacy and reputation of the SHS Trust.
- To protect the SHS Trust from legal liability
- To ensure everyone is clear about their roles in using and protecting information.
- To protect the SHS Trust's employees.
- To encourage the use of technology by providing clear guidelines on how it should be used safely across the Trust.

c. History

Version	Description	Date	Author
1.0	Initial version	September 2018	P Macallister
1.1	Reviewed	September 2019	P Macallister
1.2	Reviewed	September 2020	P Macallister
1.3	Updated	February 2021	A Gibbins
1.4	Reviewed	September 2022	P Macallister

d. Responsibilities

Roles	Responsibilities
Senior Information Risk Officer (SIRO)	• Together with Governors, liable for all aspects of the Trust's information security.
Information Security Officer	• Implement and maintain Security Policy documents. • Responsible for the security of the IT infrastructure. • Plan against security threats, vulnerabilities, and risks. • Ensure security training programs. • Ensure IT infrastructure supports Security Policies. • Respond to information security incidents. • Help in disaster recovery plans.
Information Asset Owners	• Know what information the assets hold, and what enters and leaves and why. • Know who has access and why, and ensure their use of the asset is monitored. • Understand and address risks to the asset. • Assist DPO with Subject Access Requests.
IT Team	• Implements and operates IT security. • Implements the privileges and access rights to the resources. • Supports Security Policies.
Users	• Meet Security Policies. • Report any attempted security breaches.

e. General Policy Expectations

i. Information shall be used legally at all times; complying with UK and European law.
ii. All information shall be processed in accordance with the General Data Protection Regulation, May 2018.
iii. Personal, confidential or sensitive information shall be protected appropriately at all times, especially when removed from school premises

either physically on paper or electronic storage devices, or when transmitted electronically outside the SHS Trust.

iv. Exceptions to the policies defined in any part of this document may only be authorised by the Senior Information Risk Officer. In those cases, specific procedures may be put

in place to handle requests and authorisation for exceptions.

v. Every time a policy exception is invoked, an entry must be entered into a security log specifying the date and time, description, reason for the exception and how the risk was managed.

vi. All the IT services should be used in compliance with the technical and security requirements defined in the design of the services.

vii. Breaches of information will be fully investigated.

viii. Violations of the policies in this document may lead to disciplinary actions.

2. IT Assets Policy

a. Purpose

The IT Assets Policy section defines the requirements for the proper and secure handling of all the IT assets in the SHS Trust.

b. Scope

The policy applies to desktops, laptops, printers and other equipment, to applications and software, to anyone using those assets including internal users, temporary workers and visitors, and in general to any resource and capabilities involved in the provision of the IT services.

c. Policy Assumptions

i. IT assets must only be used in connection with the business activities they are assigned and / or authorised.

ii. Every user is responsible for the preservation and correct use of the IT assets they have been assigned.

iii. Active desktop and laptops must be secured if left unattended. (i.e. users should lock their laptop or desktop screens, when they leave the room.) Whenever possible, this policy should be automatically enforced.

iv. Access to assets is forbidden for non-authorised personnel.

v. All personnel interacting with the IT assets must have been shown how to login and use the key school systems during induction. If further training is required, this should be provided preferably by the School but if not possible through outside courses.

vi. Users shall maintain the assets assigned to them clean and free of accidents or improper use. They shall not drink or eat near the equipment.

vii. Access to assets must be restricted and properly authorised, including those accessing remotely. Laptops and other equipment used at external locations must be periodically checked and maintained.

viii. The IT Team is solely responsible for maintaining and upgrading configurations. No other users are authorised to change or upgrade the configuration of the IT assets. That includes modifying hardware or installing software.

ix. Special care must be taken for protecting laptops and other portable assets from

being stolen. Be aware of extreme temperatures, magnetic fields and falls.

x. When travelling by plane, portable equipment such as laptops must remain in possession of the user as hand luggage.

xi. Whenever possible, encryption and erasing technologies should be implemented in portable assets in case they are stolen.

xii. Losses, theft, damages, tampering or other incidents related to assets that compromise security must be reported as soon as possible to the Information Security Officer.

xiii. Disposal of the assets must be done according to the specific procedures for the protection of the information. Digital assets storing confidential information must be physically destroyed in the presence of an IT Team member before disposing.

3. Access Control Policy

a. Purpose

The Access Control Policy section defines the requirements for the proper and secure handling of access to IT services and infrastructure in the SHS Trust.

b. Scope

This policy applies to all the users in the SHS Trust, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services. The policy also applies to personal information stored on paper.

c. Policy Assumptions

i. Any system that handles valuable digital information must be protected with a password-based access control system. Where appropriate, two-step verification, should be enabled.

ii. Personal information, stored on paper, must be securely stored in lockable office filing cabinets or cupboards.

iii. A discretionary access control list must be in place to control the access to resources for different groups of users.

iv. Access shall be granted under the principle of “less privilege”, i.e., each identity should receive the minimum rights and access to resources needed for them to be able to perform their business functions successfully.

v. Visitors to the Trust should be provided with ‘Guest’ login details if accessing the School network. If they are using their own equipment, and need Wi-Fi access, this must be provided by Guest Wi-Fi Access. The standard school Wi- Fi password should never be used on laptops used by visitors.

vi. Staff are discouraged from using USB sticks or SD cards without checking with IT first. No personal data should ever be downloaded and stored on such devices without encryption.

vii. Staff are not permitted to tamper or evade the access control in order to gain greater access than they are assigned.

viii. Automatic controls, scan technologies and periodic revision procedures must be in place to detect any attempt made to circumvent controls, and should also be followed up.

4. Password Control Policy

a. Purpose

The Password Control Policy section defines the requirements for the proper and secure control of passwords in the SHS Trust.

b. Scope

This policy applies to all the users in the SHS Trust, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

c. Policy Assumptions

i. Any system that handles valuable information must be protected with a password-based access control system. Where appropriate, two-step verification, should be enabled.
ii. Identities should be centrally created and managed. Single sign-on for accessing multiple services is encouraged.
iii. Each identity must have a strong, private, alphanumeric password to be able to access any service. Passwords should be at least 8 characters long.
iv. Each regular user may use the same password for no more than 90 days. The same password may not be used again for at least one year.
v. Use of administrative credentials for non-administrative work is discouraged. IT administrators must have two sets of credentials: one for administrative work and the other for common work.
vi. Sharing of passwords is forbidden. They should never be revealed or exposed to public sight.
vii. Whenever a password is deemed compromised, the Information Security Officer must be notified and the password must be changed immediately.
viii. Never use the feature 'Remember password'. If staff have done this already, they should ask the IT team to assist with removing the password memory from the browser or software used.
ix. Identities must be locked if password guessing is suspected on the account.

5. Email Policy

a. Purpose

The Email Policy section defines the requirements for the proper and secure use of electronic mail in the SHS Trust.

b. Scope

This policy applies to all the users in the SHS Trust, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

c. Policy Assumptions

The SHS Trust's email facilities should be used in a responsible manner – in particular, you must not:

i. create, transmit or cause to be transmitted material which is designed or likely to cause annoyance, inconvenience, needless anxiety or offence, and you must not create, transmit or cause to be transmitted offensive, obscene or indecent material; create, transmit or cause to be transmitted defamatory material;
ii. send any email message which is abusive, discriminatory on the grounds of sex, marital or civil partnership status, age, race, disability, sexual orientation or religious belief (or otherwise contrary to the SHS Trust's Equal Opportunities

Policy), or defamatory. Use of the email system in this way constitutes gross misconduct. The SHS Trust will take no responsibility for any offence caused by you as a result of downloading, viewing or forwarding inappropriate emails;

iii. hesitate to report somebody to the Executive Head or Heads (The Rowans and Pre-Prep), if you feel you or somebody else is being abused via the email system;
iv. conduct school business on any email other than your school email account;
v. communicate with pupils on their own personal emails, without also including their parent/guardian on the distribution of any communication with a boy;
vi. use any emoticons in any email exchanges with parents;
vii. create, transmit or cause to be transmitted material such that the copyright of another person is infringed;
viii. transmit by e-mail any confidential information of the SHS Trust otherwise than in the normal course of your duties;
ix. enter into any contract or subscription on the internet or via email correspondence on behalf of their school without authorisation from the Executive Head or Heads (The Rowans and Pre-Prep);
x. send or forward trivial messages or jokes that could cause the SHS School's IT system to suffer delays;

In addition:

i. Please be very careful when responding to emails if you need to delete any part of the attached trail before sending your reply to the recipient. Even if you delete emails or attachments on your laptop, depending on which device the recipient opens the email on e.g. certain types of iPhone, it is possible for the trail to be re-attached from the Cloud. The 'secure' approach in this instance, is to 'cut and paste' the email to which you are responding into a new mail and respond to only that email with no other trail linked to it.
ii. Identities for accessing staff email must be protected by strong passwords. The complexity and lifecycle of passwords are managed by the Trust's procedures for managing identities. Sharing of passwords is not permitted. Users should not impersonate another user.
iii. Any emails which have attachments which appear suspicious, or are from an unknown source, should not be opened under any circumstances.
iv. Where possible, attachments should not be sent to group email addresses. (i.e. sending attachments to group email addresses creates multiple copies of the attachment throughout the email system.) It is preferable that the attachments location is shared.
v. Outbound messages from SHS Trust users must have approved signatures at the foot of the message.
vi. While internal messages (e.g. within the Trust) are considered secure for personal information, external addresses are not considered secure enough for personal information.
vii. No personal information, whose disclosure could cause harm to an individual, should be sent by email, unless correct encryption procedures have been followed.
viii. Scanning technologies for virus and malware must be in place in client PCs and servers to ensure the maximum protection in the ingoing and outgoing email.
ix. Security incidents must be reported and handled as soon as possible. Users should not try to respond by themselves to security attacks.

x. Staff members are encouraged to use their laptops for all email correspondence, particularly for more complex or longer emails. Should you need to respond to an urgent email from another device, e.g. an iPad or an iPhone, you are still expected to ensure that each School's **standard sign-off** is in place.
xi. Email has a habit of being informal. If an email is to be formal, please make sure its tone reflects this. All electronic communication with parents should be formal. **This includes (other than in exceptional circumstances) when parents address staff by their Christian name or informally – please ensure that your response begins with a formal salutation.** If you require guidance on what exceptional circumstances might be, please refer to your School's handbook.
xii. Be aware that emails are disclosable as evidence in court proceedings and even if they are deleted, a copy may exist on a back-up system or other storage area.

Subject to a number of limited exceptions, potentially all information about an individual may be disclosed should that individual make a subject access request under the General Data Protection Regulation, May 2018. There is no exemption for embarrassing information (for example, an exchange of emails containing gossip about the individual will usually be disclosable). As such you must be aware that anything you put in an email is potentially disclosable.

The SHS Trust reserves the right at the behest of the Executive Head or Heads (The Rowans and Pre-Prep) or nominated Deputy to monitor and access the SHS Trust email, for purposes connected with the operation of the School. The purpose of such monitoring and access include:

i. to establish the existence of facts;
ii. to ascertain compliance with the SHS Trust's regulatory or self-regulatory procedures;
iii. to monitor standards which are achieved by persons using the system in the course of their duties and for staff training purposes;
iv. to prevent or detect crime;
v. to investigate or detect unauthorised use of the SHS Trust's system;
vi. to ensure the effective operation of the system such as protecting against viruses, backing up and making routine interceptions such as forwarding e-mails to correct destinations;
vii. to gain access to routine business communications and help the SHS Trust with its day-to-day operations, for instance checking voice mail and email when staff are on holiday or on sick leave.
viii. As there is the risk of deleting information, only the IT team, who have the expertise, should, on management's authority, access staff email.

Further Useful Guidelines

i. Show due consideration when forwarding emails of others where there may be sensitivities with potential to cause upset and, where appropriate, seek permission from the author before forwarding.
ii. If you are forwarding an email you have received, do not change the wording.
iii. Observe good housekeeping to read carefully the trail of emails attached to an email before forwarding or copying and to perhaps delete them, if they are superfluous to

the communication relating to the email.

iv. Never put anything in an email you would not put on a postcard, say to a person's face or publish generally – its contents are there for everybody to see and easier to circulate.
v. Never send chain letters via email.
vi. Contact the IT department if you consistently receive unwanted mail to ensure that appropriate action is taken.
vii. Be careful when addressing an email; an error can mean your mail going to the wrong recipient. When selecting a recipient from an address book, always double check to see you have selected the correct one.
viii. All email should have a subject message reflecting the contents of the message.

6. Internet Policy

a. Purpose

The Internet Policy section defines the requirements for the proper and secure access to the Internet.

b. Scope

This policy applies to all the users in the SHS Trust, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time to services.

c. Policy Assumptions

i. Limited access to Internet is permitted for all users. Pupils accessing the internet must always have a teacher present in the class.
ii. The use of Messenger service such as Skype is permitted for educational purposes only.
iii. Access to inappropriate sites is prohibited.
iv. Inbound and outbound traffic is filtered using LGFL's Webscreen filtering system.
v. Internet traffic is monitored using Securus XT and overseen by the IT Team. Any detections of a serious nature should be promptly reported to the Information Security Officer.
vi. As mentioned in the Email Policy, the SHS Trust does have the right to monitor and disclose staff's online history.
vii. All devices accessing the internet must be protected by anti-virus (Sophos) and Malwarebytes.

7. Mobile Policy

a. Purpose

The Mobile Policy section defines the requirements for the proper and secure use of mobile phones on SHS Trust premises.

b. Scope

This policy applies to all the users in the SHS Trust, including temporary users, visitors with temporary access to services and partners with limited or unlimited access time

to services. It applies specifically to staff who use their mobile to access school email.

c. Policy Assumptions

i. Staff using mobile phones to access school email must enable password protection on their mobile.
ii. "Find My iPhone" (Apple) or "Find My Device" (Android) must be enabled.
iii. Mobile phones (and all installed apps) should be kept up to date using the 'automatically update' option if available.
iv. Staff private mobile phones can be connected to the School Wi-Fi.
v. When sending email, don't connect to public Wi-Fi hotspots. Use 3G, 4G or 5G connectivity.
vi. Staff using mobile phones for email, must follow the guidelines in the Email Policy.
vii. Pupils are not allowed to use mobiles at school. All pupil mobiles should be handed to reception for safe keeping during school hours.

8. Antivirus Policy

a. Purpose

The Antivirus Policy section defines the requirements for the proper implementation of antivirus and forms of protection in the SHS Trust.

b. Scope

This policy applies to servers, workstations and equipment across the SHS Trust, including portable devices like laptops that may go home with a teacher. Some policies apply to external computers and devices accessing the resources of the School.

c. Policy Assumptions

i. All computers and devices with access to a school's network must have an antivirus client installed, with real-time protection.
ii. All the installed antivirus must automatically update their virus definition. They must be monitored to ensure successful updating is taken place.
iii. Visitor computers and all computers that connect to the School's network are required to have a valid, updated antivirus software installed.

9. Information Classification Policy

a. Purpose

The Information Classification Policy section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality and availability of the SHS Trust's information.

b. Scope

This policy applies to all the information created, owned or managed by the SHS Trust, including those stored in electronic or magnetic forms and those printed in paper.

c. Policy Assumptions

i. Information asset owners must ensure the security of their information and the systems that support it.

ii. Any breach must be reported to the Information Security Officer immediately. If needed, the appropriate countermeasures must be activated to assess and control damages.

iii. Information in the SHS Trust is classified according to its security impact. The current categories are: confidential, restricted, internal use and public.

- Information defined as **confidential** has the highest level of security. Only those who explicitly need access to the information should have access, and only to the least degree in order to do their work. Data defined by the GDPR as ***Special Categories of Personal Data*** falls into this category.
- Information defined as **restricted** should only be accessed by SHS Trust staff via login. Data defined by the GDPR as ***Personal Data*** falls into this category.
- Information defined as **internal use** should only be accessible to the SHS Trust staff at their respective schools. Information in this category includes: internal correspondence and minutes etc.
- Information defined as **public** can be accessed by all members of the public, e.g. content published on each school's website.

iv. Information is classified jointly by the Information Asset Owner and the Data Protection Officer.

10. Remote Access Policy

a. Purpose

The Remote Access Policy section defines the requirements for the secure remote access to the SHS Trust's internal IT resources.

b. Scope

This policy applies to the users and devices that need access to the SHS Trust's internal resources from remote locations.

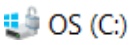
c. Policy Assumptions

i. To gain access to the school network from remote locations, users must have the LGFL Freedom2Roam AnyConnect Client set up on their laptops.

ii. The password must have multi-factor authentication enabled. Staff need to enter their password followed by a dot and their 6-digit Google Authenticator code to access the VPN.

iii. No personal data should be downloaded to a laptop's hard drive. Users should log into their school VPN and access their files in this way.

iv. All devices (laptops), used to access the SHS Trust's IT network remotely, must have their hard drive encrypted. Staff can check that their hard drive is encrypted by looking for an open lock on the C: Drive in File Explorer – see below:



If the lock does not show, then staff should check with IT support.

11. Outsourcing Policy

a. Purpose

The Outsourcing Policy section defines the requirements needed to minimise the risks associated with the outsourcing of IT services, functions and processes.

b. Scope

This policy applies to the SHS Trust; the service providers to whom IT services, functions or processes are being outsourced, and the outsourcing process itself.

c. Policy Assumptions

i. Before outsourcing any service, function or process, a careful strategy must be followed to evaluate the risk and financial implications.
ii. Whenever possible, a bidding process should be followed to select between several service providers.
iii. In any case, the service provider should be selected after evaluating their reputation, experience in the type of service to be provided, offers and warranties.
iv. Audits should be planned in advance to evaluate the performance of the service provider before and during the provision of the outsourced service, function or process. If SHS Trust has not enough knowledge and resources, a specialised company should be hired to do the auditing.
v. A service contract and defined service levels must be agreed between the SHS Trust and the service provider.
vi. The service provider must get authorisation from the SHS Trust if it intends to hire a third party to support the outsourced service, function or process.

12. Annex

a. Glossary

Term	Definition
Access Management	The process responsible for allowing users to make use of IT services, data or other assets.
Asset	Any resource or capability. The assets of a service provider include anything that could contribute to the delivery of a service.
Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, that records are accurate, or that efficiency and effectiveness targets are being met.
Confidentiality	A security principle that requires that data should only be accessed by authorized people.
External Service Provider	An IT service provider that is part of a different organisation from its customer.
Identity	A unique name that is used to identify a user, person or role.
Information Security Policy	The policy that governs the organization's approach to information security management
Outsourcing	Using an external service provider to manage IT services.

Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of processes, standards, roles, activities, IT infrastructure etc.
Risk	A possible event that could cause harm or loss, or affect the ability to achieve objectives.