SIR WILLIAM PERKINS'S SCHOOL

IT ACCEPTABLE USE

1. Policy Statement

Sir William Perkins's School makes use of Information Technology as part of its teaching, learning, and business operations. Misuse of the school's IT devices, facilities, or services in a way that constitutes a breach or disregard of this policy may also constitute a breach of other school policies.

This purpose of this policy is to:

- Ensure the integrity of the school's network and its equipment
- Ensure that school data is secure
- Ensure that staff and students are protected from activities that may expose them to harm

In line with the Independent School Standards Regulations (ISSR) for the Welfare, Health and Safety of Pupils, this policy forms part of the School's guidance on the use of technology in the classroom and beyond for all users, including staff, students and visitors.

SWPS is fully committed to ensuring that the application of this policy is non-discriminatory, in line with the UK Equality Act (2010). Further details are available in the school's Equal Opportunities policy.

2. Scope

All IT hardware, software, networks, telephony, communications, digital platforms, and online services that that the School owns, operates, or uses are covered by this policy.

3. Responsibilities

All users hold a level of responsibility in maintaining the integrity of the School's network, to ensure it can continue to be used safely and effectively.

It is a requirement that all users have read and understood the contents of this policy and signed to accept its content before accessing any of the School's IT devices, facilities, and services. Failure to do so may result in the user's access being suspended or withdrawn.

The policy should be read in conjunction with the following school documents:

- E-safety Policy
- Student Device Policy
- Staff Device Policy
- Shared Device Policy

4. Acceptable Use

Sir William Perkins's School defines acceptable use as activities that directly or indirectly support the operation of school and the education of its students. The primary uses of the school's IT devices, facilities, and services should be for study, research, teaching, and administration of the school.

The school allows for limited personal use of IT equipment or services as long as the use is reasonable in nature and limited to time outside that which spent teaching or completing other work requirements.

5. Misuse

Sir William Perkins's School will not tolerate use of the School's IT devices, facilities, or services for illegal activities or activities that are inappropriate in a school context. They must NOT be used at any time to:

- Access, create, store, display, transmit, or distribute, any offensive, obscene, indecent, threatening, or illicit images, data, or materials.
- Store, transmit, or distribute any personal private data.
- Conduct any form of unauthorised commercial activity or financial trading.
- Initiate or participate in malicious scans, probes, attacks, or other unauthorised system access.
- Install or distribute any software or service without licence, and any that is not authorised by the IT department.
- Harass, defame, libel, slander, intimidate, impersonate or abuse any another person.
- Disseminate unsolicited mass mailings.
- Disrupt or interfere with any others use of the School's devices, facilities, and services.
- Engage in activities which might damage the reputation of the School or bring it into disrepute.

Where the School has reasonable grounds to suspect misuse has taken place, it reserves the right to record and review the source, destination, length, nature, and content of:

- Calls made on School phones.
- Websites and digital services accessed from the School network.
- School emails and other digital communications.
- Data stored on School-owned devices.

Such records are sometimes required by law to be submitted to external authorities, and the School will comply with any formal requests submitted.

6. Use of Equipment

All users of IT equipment must adhere to the following rules at all times:

- Treat all School equipment safely and responsibly.
    - Keep liquids away from the equipment.
    - Do not drop, throw, or otherwise mishandle the IT equipment.
- Devices must either be carried on person or physically locked away when not in use.
- Extra care must be taken to prevent the loss of USB drives or portable equipment which contain School data.
- Staff supervising students using IT equipment are responsible for ensuring that they take reasonable care of equipment.

If School equipment has been lost, stolen, or damaged in any way, you must notify the IT department immediately.

7. Accounts and Passwords

Access to most devices, systems, and services is controlled by an account and password. It is the responsibility of all users of the School's IT devices, facilities, and services to adhere to the following requirements for passwords or access codes:

a) Passwords and access codes must never be written down on hard-copy.
b) Passwords and access codes must not be inserted into emails or other forms of electronic communication.

c) Passwords and access codes stored digitally should be encrypted.
d) Passwords and access codes must not be revealed to other users or shared with them.
e) Passwords and access codes must not be re-used on multiple platforms or services.
f) Passwords and access codes used at School must not be used for personal services, and vice versa.
g) All passwords must conform to these complexity requirements:
    - Contains a minimum of 12 characters
    - Contains at least three of these four categories: Uppercase, Lowercase, Number, Symbol
h) Passwords must NOT contain any of the following:
    - Identifying information (names, birthdays, phone numbers)
    - Common use words and phrases (pets, fantasy characters etc.)
    - Computer terms (password, login, laptop)
    - Word or number patterns (qwerty, 12345 etc.)

Users must not leave unlocked devices unattended, to prevent unauthorised access to School systems or data by any other staff, students, or members of the public.

If users believe that someone knows their password, or their account has been compromised in any way, they must change their password immediately and report the matter to the IT department.

8. Multi-Factor Authentication

Multi-Factor Authentication makes use of a digital token on a physical device to ensure that a compromised password alone cannot be used by a malicious actor to gain access to the School network.

Users may be required to store this token on a personal device, such as a mobile phone, by installing an authenticator app. In doing so, no School data is stored on the personal device, and no control, visibility, or ownership over the device is granted to the School.

9. Data Security

The School holds a variety of sensitive data including personal information about students and staff. If you have access to any of this information as part of your role, you are reminded of your responsibilities under data protection law.

Personal identifying information or business sensitive data should be accessed in-situ on School systems. Copies of School data should not be taken out of the School's systems, except where all other options have been exhausted, and when explicitly authorised by a member of the Senior Leadership Team. This includes putting data onto any removal media (USB drives, CDs, SD Cards etc.), onto any personal devices, or in personal emails. All removable media taken off School site, or sent by post or courier, must have its content encrypted.

Staff and students are advised to contact the IT department if you are unsure about any aspect of data security, or to report any suspected data or security breach.

10. Devices

All School owned machines are protected by the latest updates, use of firewalls, and up-to-date enterprise versions of virus and ransomware software. These are used to prevent attacks from malicious actors and protect from loss of data, and corruption or control of programs/files.

Staff, students and visitors at Sir William Perkins's School are permitted to bring personal devices onto School site for their own use providing their usage does not interfere with the School day, and is in line with acceptable use.

When a personal device is not in use it should be locked to prevent unauthorised access by other users. The School holds no responsibility for the loss, damage, or theft of any personal devices.

It is the responsibility of the user to ensure that any personal-owned device connecting to the School's network has the latest updates installed and is running up to date anti-virus software. Any devices which are flagged by the School's security as acting in a malicious manner, or behaving abnormally due to possible viral infection, will be blocked from the School network and will not granted access again until the device has been confirmed as clean by School IT staff.

11. Use of Emails

Any School-related communications must be sent via School email or other School communication service. Personal emails must not be used to communicate with other staff, students, parents, or the public about any official School matters.

School emails must not be automatically or frequently forwarded to an external address for the express purpose of accessing or storing School emails outside of School systems.

Emails with sensitive content should be sent encrypted, and the decryption key sent via an alternative means of communication, such as text message, or over the phone.

Users should be careful that, before they open any attachment on an email they receive, they are reasonably confident that the content is not malicious in nature, and is in no sense illicit, obscene or defamatory. Equally, if a user receives a malicious, illicit, obscene or defamatory email or attachment, whether unwittingly or otherwise, and no matter the source, they should not intentionally copy or forward the email to any other address unless specifically requested to do so by an investigator appointed by the School.

Email should be treated like any other form of written communication, and as such, should only contain content that would also be viewed as acceptable in a physical letter or memorandum.

Employees must exercise caution when sending an email from a School address to any external address, ensuring that the recipient is correct and the content is appropriate, as the email cannot be recalled.

12. Use of the Internet

All internet browsing is proactively monitored for misuse. Users will be blocked from accessing categories of inappropriate websites whilst connected to the School network. The School has a zero-tolerance policy for the use of devices to visit banned websites, including attempts to visit illicit material which are successfully blocked.

13. Remote Access

Remote access to the School network is possible where this has been set up and access granted by the IT department. Remote connections are considered direct connections to the School network, and as such, using these services remotely subjects the user to the same conditions, requirements, and responsibilities set out in the rest of this policy.

It is the responsibility of users of remote access to ensure that unauthorised users are not allowed to access the School's internal network by means of sharing the connection.

14. Delegate Access

The School reserves the right to delegate the access of user files and e-mails to another user holding a management role, or in the event of unexpected or prolonged absence (e.g. due to sickness), during maternity/paternity leave, or on the user's final departure from the School.

15. VPNs

Policies are in place to restrict the use of VPNs on the School network accessing the internet. All users are forbidden from using VPNs both on School-owned devices, and on personal devices whilst connected to the School network to ensure safeguarding of staff and students.

16. Wireless

Users are forbidden from creating, using, or providing, personal wireless networks in proximity to the School site, with the aim of disrupting School wireless systems, or circumventing web filtering. Non-standard, misconfigured, or malicious wireless devices causing interference may be seized.

17. Agreement

By signing a copy of this policy, the user accepts that a breach of its rules may result in disciplinary or legal action, and that non-compliance or negligence may require the user to make a full or partial contribution towards any reparation/replacement costs, at the discretion of the School.

18. Monitoring and Review

The Governing Body is ultimately responsible for the effective oversight, review and amendment of this policy and understands its legal obligation to do so.

This document will be reviewed and updated annually by the School's IT Manager in consultation with Assistant Head Digital Strategy, or as events or legislation requires.

Next scheduled review date: 04/2025 Last reviewed: 04/2024	
Key updates in this version:	• Change to primary policy reviewer as IT Manager • Updates to job titles • Minor formatting updates for clarity