Acceptable Information Technology (IT) & Internet Use policy (including mobile phones and social media)

The Sheriff Partnership

Home of Coventry and Central Warwickshire Teaching School Hub

Review date	Autumn 26
Review period	Annual by SLT Triennial by Pastoral Committee
Next Review date	Autumn 27
Reviewed by	N Dandy
Approving committee	Pastoral Committee
Policy type	Non legislative
Other related policies	Online safety policy Child protection & Safeguarding policy Behaviour policy Staff code of conduct GDPR / Data protection

Contents

1. Introduction and aims 2
2. Relevant legislation and guidance 2
3. Definitions 3
4. Unacceptable use 3
5. Staff (including trustees, volunteers, and contractors) 4
6. Pupils 8
7. Parents/carers 11
8. Data security 12
9. Protection from cyber attacks 13
10. Internet access 14

Appendix 1: Facebook / Social Media Guidelines for staff 16

Appendix 2: Glossary of cyber security terminology 19

Appendix 3 – Home School Laptop agreement 21

Appendix 4 - Acceptable Use of IT Agreement (Students) 23

Appendix 5 - LAWRENCE SHERIFF SCHOOL BYOD 6TH FORM STUDENT WIFI APPLICATION 25

Appendix 6: Acceptable use of AI for pupils and staff 26

1. Introduction and aims

Information technology (IT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), trustees, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the IT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school IT resources for staff, pupils, parents/carers and trustees.
- Establish clear expectations for the way all members of the school community engage with each other online.
- Support the school's policies on data protection, online safety and safeguarding.
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of IT systems.
- Support the school in teaching pupils safe and effective internet and IT use.

This policy covers all users of our school's IT facilities, including trustees, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under the school's staff code of conduct, or in the case of pupils, the school's behaviour policy.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **IT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's IT service.
- **Users:** anyone authorised by the school to use the school's IT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user.
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the IT facilities.
- **Materials:** files and data created using the school's IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

See appendix 2 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's IT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's IT facilities includes:

- Using the school's IT facilities to breach intellectual property rights or copyright.
- Using the school's IT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's policies or procedures.
- Any illegal conduct, or statements, which are deemed to be advocating illegal activity.
- Using inappropriate or offensive language.
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.
- Online gambling, inappropriate advertising, phishing and/or financial scams.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful.
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, its pupils, or other members of the school community.
- Connecting any device to the school's IT network without approval from authorised personnel.
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's IT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities.
- Causing intentional damage to the school's IT facilities.
- Removing, deleting or disposing of the school's IT equipment, systems, programmes or information without permission from authorised personnel.

- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation.

- Students and staff must ensure that all personal and sensitive data is handled securely and in compliance with school policies and data protection laws. Any data breaches, including unauthorised access, sharing, or loss of school or student information, must be reported immediately to the DPO. Additionally, while Artificial Intelligence (AI) tools can be valuable for learning, they should be used responsibly. AI-generated content must be properly reviewed, and students should not rely on AI for unethical purposes such as plagiarism or bypassing academic integrity.

- Promoting a private business, unless that business is directly related to the school. Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms. Using AI tools and generative chatbots (such as ChatGPT and Google Bard) to plagiarise work; this could include using AI tools:
    - during assessments, including internal and external assessments, and coursework.
    - to write their homework or class assignments, where AI-generated text or imagery is presented as their own work.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher, members of SLT or the Pastoral team will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's IT facilities.

4.1 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's behaviour policy and staff code of conduct. The headteacher reserves the right to impose of temporary ban, where appropriate, if a pupil misuses an IT device connected to the school network. Mobile phones are not permitted to be used by pupils in Years 7 -11 during the school day and are confiscated if they are seen during these times, unless under the specific occasional instruction from a member of staff. Sixth Form pupils are permitted to use mobile phones for educational purposes within the Sixth Form centre or during lessons, if directed by a member of staff.

5. Staff (including trustees, volunteers, and contractors)

5.1 Access to school IT facilities and materials

The school's Director of IT Services manages access to the school's IT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices.
- Access permissions for certain programmes or files.

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's IT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Director of IT Services.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers and pupils, and should not send any work-related materials using their personal email account.
Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not necessarily mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the school's Data Protection Lead immediately and follow our data breach procedure.

Staff must take care when using AI tools such as Chat GPT or Google bard not to upload any personal data relating to individual students, staff or school business, such as student names, email addresses.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff should, if possible, use phones provided by the school to conduct all work-related business. If this is not possible then staff should ensure that their caller ID is turned off and no personal or sensitive data (i.e. parent phone numbers) are inadvertently stored on their mobile phone or device.

School phones should not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for IT acceptable use, as set out in section 4.

5.2 Personal use

Staff are permitted to occasionally use school IT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The headteacher may withdraw or restrict this permission at any time and at their discretion. Any safeguard concerns that arise are dealt with by the Headteacher/DSL/Deputy DSL.

Personal use is permitted provided that such use:

- Does not take place during teaching hours or whilst undertaking duties which involve the supervision of pupils.

- Does not constitute 'unacceptable use', as defined in section 4.
- Takes place when no pupils are present.
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes.

Staff may not use the school's IT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's IT facilities for personal use may put personal communications within the scope of the school's IT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets).

Staff should be aware that personal use of IT / social media (even when not using school IT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (see appendix 1) in accordance with the staff code of conduct and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook / social media accounts (see appendix 1).

5.3 Remote access

Staff may have access to the school's IT facilities and materials remotely. They should dial in using a secure private WIFI connection. Staff can either use the laptop with which they have been provided or their own device. If the device is shared then appropriate GDPR should be practiced to ensure the school data is not viewable by anyone else that uses the shared device. Remote access is via our paid for multifactor authentication (MFA) portal linked to our Microsoft Welearn365 accounts.

This system is hosted by the Warwickshire ICTDS Service Desk team. It is managed in part by the ICTDS team and LSS IT administrators. Any member of staff that needs access remotely must have access to an app capable smart device. Once approval has been granted, the LSS IT team will forward the necessary details to the ICTDS team to allow or permit access to the multifactor authentication system. After confirmation that access has been granted the member of staff will be given a document on how to setup their MFA app device and remotely access the school network.

Staff accessing the school's IT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's IT facilities outside the school and must take such precautions as the Director of IT Services may require against importing viruses or compromising system security.

Our IT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

5.4 School social media accounts

The school has an official Instagram account, managed by a Deputy Headteacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines (see appendix 6) for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.5 Monitoring and filtering of the school network and use of IT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its IT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited.
- Bandwidth usage.
- Email accounts.
- Telephone calls.
- User activity/access logs.
- Any other electronic communications.

Only authorised IT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The school's internet is provided by the Local Authority (Warwickshire) and as such they provide the school's filtering and monitoring services. Warwickshire County Council's ICT Development Service (WCC ICTDS) manages IT systems for schools within Warwickshire. This network monitors 45,000 staff and pupils across the county, including all staff and pupils at Lawrence Sheriff School. WCC ICTDS uses Smoothwall Filter Solution to provide monitoring and filtering for all of its schools.

Subsequently, the school uses this to ensure that all members of the school community are able access online material safely. Smoothwall blocks and proactively monitors harmful or dangerous content without over blocking, ensuring that pupils and staff are able to continue learning whilst safety explore the internet. These meet the Government Standards for Filtering and Monitoring 2023 and the requirements of Keeping Children Safe in Education 2023. The filtering and monitoring provision is managed by the school's Director of IT services who works together with the Designated Safeguarding Lead to regularly monitor and ensure that the system is operating effectively.

The school monitors IT use in order to:

- Obtain information related to school business.
- Investigate compliance with school policies, procedures and standards.
- Ensure effective school and IT operation.
- Conduct training or quality control exercises.
- Prevent or detect crime.

- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

Our Trust Board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place.
- Staff are aware of those systems and trained in their related roles and responsibilities.
- Ensure the leadership team and relevant staff, will know how to manage the processes and systems effectively and how to escalate concerns.
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.
Where appropriate, staff may raise concerns about monitored activity with the school's DSL and Director of IT Services, as appropriate.

6. Pupils

An 'Acceptable Use of IT Agreement Form' (appendix 4) is shared with all parents / carers and pupils when they join the school. This clearly outlines the rules and expectations of pupils when using IT. As part of the induction process, all Year 7 and 12 pupils are taught how to use IT responsibly and safely, in line with this policy and our Online Safety policy. Under certain circumstances, pupils may be given access to a school device to use at home. In these situations, pupils and parents agree to the Laptop User Agreement (appendix 3) and must adhere to the same rules and principles as outlined in our Acceptable Use of IT Agreement Form.

6.1 Access to IT facilities

- Computers and equipment in the school's IT suite are available to pupils only under the supervision of staff.
- Specialist IT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.
- Sixth-form pupils can use the computers independently, for educational purposes only.

6.2 Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Possess a risk to staff or pupils.
- Are identified in the school rules as a banned item for which a search can be carried out - Searching Students and Restraint by Staff Policy.
- Are evidenced in relation to an offence.

This includes, but is not limited to:

- Pornography.
- Abusive messages, images or videos.

- Indecent images of children.
- Evidence of suspected criminal behaviour (such as threats of violence or assault).

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / deputy headteacher.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's co-operation.
- The authorised staff member should inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available via the school's Searching Students and Restraint by Staff Policy.
- Involve the DSL (or deputy DSL) without delay if they believe that a search has revealed a safeguarding risk.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a school device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- cause harm, **and/or**
- undermine the safe environment of the school or disrupt teaching, **and/or**
- commit an offence

If inappropriate material is found on the device, then the headteacher will work with the school's DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- they reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- the pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **not** view the image
- **not** copy, print, share, store or save the image

- confiscate the device and report the incident to the DSL (or deputy DSL) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with the same guidance above and:

- the school's Behaviour Policy / Searching Students and Restraint by Staff Policy
- any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Acceptable use of AI

We recognise the growing role of Artificial Intelligence (AI) in education and everyday life. While AI can be a valuable tool for learning and creativity, it also presents potential risks.

Students must:

- Use AI responsibly and ethically when given permission to do so.
- Copilot Chat (for education) is the only AI tool permitted for use in school by staff or students.
- Copilot chat does not require parental permission and is to be used by age 13 plus only (not to be use by year 7 and 8)
- Be aware of the risks of misinformation, bias, and privacy concerns when using AI-generated content.
- Not use AI tools to cheat, plagiarise, or complete assignments dishonestly.
- Never share personal or sensitive information with AI systems, as data security cannot be guaranteed.
- Seek guidance from teachers before using AI tools for schoolwork.

The school will:

- Educate students about the benefits and risks of AI.
- Monitor AI-related activities to ensure safe and age-appropriate use.
- Take disciplinary action if AI is used inappropriately or to compromise academic integrity.

6.4 Unacceptable use of IT and the internet outside of school

The school retains the right to sanction pupils, in line with the behaviour policy if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using IT or the internet to breach intellectual property rights or copyright.
- Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the school's IT policies or procedures when using school loaned equipment.
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery).
- Activity which defames or disparages the school, or risks bringing the school into disrepute.

- Sharing confidential information about the school, other pupils, or other members of the school community.
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's IT facilities.
- Causing intentional damage to the school's IT facilities or materials.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.

6.5 Use of mobile phones, smart watches or other mobile smart devices

- Mobile phones/smart watches or other mobile smart devices must not be used by students in Years 7-11 during the school day (8:45am – 3:30pm). They must be secured in bags and not in trouser or blazer pockets. There are no exceptions to this.
- Sixth Form students can use their mobile phone/mobile devices in the Sixth Form Centre common room only or under the supervision and direction of a member of staff. There are no exceptions to this.
- If a student is found using a mobile phone, smart watches or other mobile smart devices, when they should not, they it will be confiscated overnight in the first instance in line with the school behaviour policy. If a phone needed to be confiscated a second time the period of time will increase and parents may be asked to come into school and collect the phone.
- Any student in school, or involved in school activities, using a mobile phone to upload/share inappropriate material, will be subject to significant disciplinary sanctions.

7. Parents/carers

7.1 Access to IT facilities and materials

Parents/carers do not have access to the school's IT facilities as a matter of course.

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

7.3 Communicating with parents/carers about pupil activity

The school will notify parents and carers, as appropriate, of any online activity that their children are being asked to carry out.

When the school asks pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, Lawrence Sheriff will inform parents / carers of the identity of any person, or people, from the school, that pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.
Staff, pupils, parents/carers and others who use the school's IT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls.
- Security features.
- User authentication and, where appropriate, multi-factor authentication.
- Anti-malware software.

8.1 Passwords

All users of the school's IT facilities should set strong passwords for their accounts and keep these passwords secure.
Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

8.2 Software updates, firewalls and anti-virus software

All of the school's IT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's IT facilities.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

8.4 Access to facilities and materials

All users of the school's IT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the Director of IT Services.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Director of IT Services immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 Encryption

The school makes sure that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Director of IT Services.

9. Protection from cyber attacks

Please see the glossary (appendix 2) for cyber security terminology.

The school will:

- work with Trustees and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security
- make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- investigate whether our IT software needs updating or replacing to be more secure
- not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- put controls in place that are:
    - **Proportionate**: the school will verify this using a third-party audit (360 degree safe) to objectively test that what it has in place is effective.
    - **Up to date:** with a system in place to monitor when the school needs to update its software.
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be.

- Back up critical data. IT systems are backed up daily by the Local Authority (Warwickshire) and these backups are stored on a cloud based system outside of the school network
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the Local Authority (Warwickshire)
- Make sure IT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test a cyber incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed annually or after a significant event has occurred.
- Work with our Local Authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The school's wireless internet (WiFi) connection is secure. The school has various wireless internet connections. All connections are ultimately secure. Any insecure networks are onboarding gateways for accessing the secure connections.

All secure networks are linked to a Smoothwall internet filter. Depending on the connection this is either managed by the school or the ICTDS Service Desk Only the filter managed by the school's IT team can be modified.

Currently the school WiFi is for staff and student internally managed laptops, administration devices, one day visitors, and Sixth Form Bring Your Own Device (BYOD). The Sixth Form WiFi is controlled using Ruckus Cloudpath, removing the need for WiFi passcodes that can be extracted from any device. The onboarding gateways are only available following a Sixth Form BYOD request. Visitor WiFi codes are changed daily.

The internet access is externally monitored by the ICTDS Service Team. Anyone attempting to bypass the school internet filter or obfuscate their connection activities with a VPN may have their access privileges terminated. This may lead to a permanent ban from the school network and / or Police action may be taken.

Any inappropriate websites that manage to get through the filters should be reported to the school's IT team or a member of SLT. This will be reviewed, and the appropriate steps taken to block the content.

10.1 Pupils

Bring Your Own Device is only available to LSS Sixth Form pupils, as it is not permissible for pupils in Years 7 -11 to use their own personal device during the school day. This provision is currently limited to Windows devices only. The BYOD WiFi covers the entire main site, but not our remote sports facility.

The WiFi is filtered using Smoothwall. Privacy mode on modern devices will need to be disengaged to work with the WiFi.

Pupils can request access to the BYOD WiFi by obtaining a request form or filling out an online Google Form (appendix 5) via the Head of Sixth Form. The LSS IT team will review each request and will contact the student to arrange connecting their device to the BYOD WiFi.

The use of the WiFi is strictly for necessary educational purposes only. It is not for social media, playing games, watching movies, or other leisure activities. All other IT Acceptable Use rules (appendix 4) also apply to this WiFi access.

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the Director of IT Services.

The Director of IT Services will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PA).
- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).

Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Appendix 1: Facebook / Social Media Guidelines for staff

Inappropriate use of social media/internet

The following list is non-exhaustive. It is intended to provide some examples of what the School considers to be inappropriate. Each matter will be dealt with based on its own facts. School policies will be followed where relevant. The school will contact the Police where it is necessary to do so.

- Publishing defamatory; discriminatory; illegal; sexual; racist or other offensive material;
- Publishing any material which is confidential or would breach copyright or data protection principles;
- Promoting personal financial interests, commercial ventures or personal campaigns in school time;
- Publishing anything of an abusive or harassing nature;
- Using social media/internet sites in a manner that would put staff/governors in breach of school codes of conduct or existing policies;
- Discussing matters relating to school, staff, pupils or parents/carers for which the social media is not considered to be an appropriate forum;
- Inappropriately holding yourself out as, or implying that you are, a representative of the school when using social media/internet sites in a private context;
- Interacting with pupils via social media/internet sites [unless properly authorised as part of school duties];
- Interacting with any ex-student who is under the age of 18 (staff should exercise extreme caution in interacting with any ex-pupils regardless of age);
- Actively providing false or misleading information about the school, its staff or pupils;
- Cyber-bullying;
- Inappropriately referencing other staff members, Trustees, students, parents or school activities/events - unless it is a legitimate part of the staff member's role;
- Using social media/internet sites to raise complaints/grievances – any issues should be raised via the appropriate channels (e.g. school complaints procedure).

Ten guidelines for school staff on Facebook / Social Media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Don't share anything publicly that you wouldn't be happy showing your pupils.
6. Don't use social media sites during school hours.
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there.
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event).
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information.

10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils).

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list.
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts.
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster.
- **Google your name** to see what information about you is visible to the public.
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this.
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile.
- Check your privacy settings again, and consider changing your display name or profile picture.
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages.
- Notify the senior leadership team or the headteacher about what's happening.

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school.
    - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in.
    - If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so.

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way.
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred.
- Report the material to the relevant social network and ask them to remove it.
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents.

- If the perpetrator is a parent/carer or other known external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material.
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police.

Appendix 2: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate

TERM	DEFINITION
	website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

Appendix 3 – Home School Laptop agreement

Lawrence Sheriff School

Lawrence Sheriff - Student Laptop (Loan)

USER AGREEMENT

I acknowledge receipt of the following equipment:

1. LSS laptop PC and power lead.

I understand that I am the named individual for the above equipment and recognise that I am responsible for ensuring that it is kept securely and used appropriately at all times. I also understand and accept that:

1. The ownership of the equipment remains with the school and I will return the device when asked
2. The equipment is to be used solely for the purpose of learning and in accordance with the terms of the Student Acceptable Use Agreement.
3. The equipment is only insured under the school policy when in school (it must be in a secure place when left unattended).
4. The laptop is **not** insured in transit and specifically if left in a motor vehicle – **the school is not liable for any loss.**
5. The school **is not obliged** to replace laptops, batteries, and power packs that are lost or damaged beyond repair.
6. I am expected to take additional sensible precautions to ensure the safety of the equipment when left unattended.
7. I should only use the supplied power pack with the laptop and if a replacement is required it should be pre-approved by the Director of IT Services.
8. I will reimburse the school for any damage to the laptop or power lead

I understand and accept that I have a role to play in ensuring the security of any essential IT equipment that is installed and that:

1. I should take all reasonable steps to ensure the security of the equipment.

2. I should allow no opportunities for any other persons to tamper or use the equipment for other than the purpose of learning.

3. I am responsible for reporting any problems with the laptops to the Director of IT Services or IT Technician as soon as possible.

Name of student: _____

signature: _____

Date: _____

Name of Parent: _____

signature: _____

Date: _____

Appendix 4 - Acceptable Use of IT Agreement (Students)

As part of the school's IT programme, we offer pupils access to school computers and to the Internet. Before being allowed to use these resources, all pupils must obtain parental permission and both they and you are requested to sign the Confidential Personal Information Sheet as evidence of your approval and their acceptance of the school rules on this matter.

Access to the Internet enables pupils to explore thousands of libraries, databases and forums while exchanging messages with other Internet users throughout the world. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. Lawrence Sheriff School does not condone the use of such materials and will use its best endeavours to prevent access to all such inappropriate materials.

Whilst our aim for computer use and Internet use is to further educational goals and objectives, pupils may find ways to access other materials as well. We believe that the benefits to pupils from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. But ultimately, parents and carers of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the school supports and respects each family's right to decide whether or not to apply for access.

During school, teachers will endeavour to guide pupils towards appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

We should be grateful if you would read the following guidance notes and then complete relevant section on the personal information form and return it with your acceptance papers - **if permission is not given, pupils will be barred from using the computer network and the Internet**. If you do not wish your son/daughter to have access to the Internet, please would you confirm this in writing.

Pupils will be provided with a personal Gmail account which will be used by them to communicate with teachers and fellow pupils. This account should not be used by parents to communicate with the school.

SCHOOL RULES ON THE USE OF COMPUTERS AND THE INTERNET

- Pupils are responsible for good behaviour on the school computers and the Internet just as they are in a classroom or a school corridor. General school rules apply.
- The Internet is provided for pupils to research classroom projects and communicate with others (E-mail). Parents' permission is required. Remember that access is a privilege, not a right and that access requires responsibility.
- Individual users of computers and the Internet are responsible for their behaviour and communications over the network. It is presumed that users will comply with school standards and will honour the agreements they have signed.
- Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or disks would always be private.
- Pupils are expected to make best endeavours to ensure malicious code is not introduced onto the computers in the school.
- Pupils should logon using only their own school logon information (do not use logon information belonging to someone else) and should not divulge personal logon details to others.
- Pupils should not use computers in any way that is deemed by the school now or in the future, to be detrimental to others or to the smooth running of the school's computer infrastructure.

The following are not permitted:

1. Sending or displaying offensive messages or pictures.
2. Using obscene language.
3. Harassing, insulting or attacking others.
4. Damaging computers, computer systems or computer networks.
5. Violating copyright laws or copying/pasting others' work without noting the source.
6. Bringing into school, in electronic form, any materials that would be unacceptable on paper.
7. Intentionally wasting limited resources.
8. Using the Internet for any illegal purpose.

Please note this list is not exhaustive. For a full and comprehensive list of unacceptable use of IT, then please refer to the school's 'Acceptable Information Technology (IT) & Internet Use Policy'

Sanctions:

1. Violations of the above rules will result in a temporary or permanent ban on network and Internet use.
2. Additional sanctions may be added in line with existing practice for inappropriate language or behaviour.

Appendix 5 - LAWRENCE SHERIFF SCHOOL BYOD 6TH FORM STUDENT WIFI APPLICATION

Guidelines:

- Students participating in B.Y.O.D. must adhere to the Acceptable Use of IT Agreement (Students).
- Students are responsible for their own device; the school accepts no liability for damage, loss or theft.
- Students are responsible for ensuring their device is suitably charged. Due to health & safety reasons, students do not have permission to charge their device at school.
- A device must only be used for educational purposes as outlined in the Acceptable Use of IT Agreement (Students).
- Each teacher has the discretion to allow and regulate the use of devices in the classroom and on specific projects. Members of staff reserve the right to confiscate a device which is being used inappropriately.
- The device must be running original and legal copies of the operating system and any other software or app. If they are not original and legal copies, then they should not be connected to the school network. Approved devices must be in silent mode while on school grounds, unless otherwise allowed by a teacher. Headphones may be used with teacher permission.
- Devices may not be used to contravene exam conditions be they internal or external assessment.
- Devices must not be used to record, capture images, video or audio of other students or staff without their consent. Images, video or audio must not be shared or posted on a social media site without the consent of those involved.
- Devices may only be used to access computer files on internet sites which are relevant to the classroom curriculum.
- Fair use of the school network is permitted during school hours, however the following are not permitted and not limited to: downloading of illegal or copyrighted material, use of streaming websites, any method to obfuscate internet usage, and use of a device and the school network to abuse others or circulate unsuitable material is also unacceptable.

DECLARATION

I confirm that I have read and understood the Acceptable Use IT Agreement and will adhere to the guidelines set out above. I hereby declare that I shall use the WiFi access allocated to me as per the existing policies of Lawrence Sheriff School IT facilities. I shall not reveal my WiFi Credentials to anyone, will not use Proxies or VPN's to mask my internet usage, and I am solely responsible for the activities done through my internet access. I acknowledge that this WiFi is the property of the local authority who reserve the right, as part of their Safeguarding and Prevent obligations, to monitor all traffic from this device when using their WiFi connection. Any misuse may result in permanent disqualification from using this service.

Signature: **Date:**

PRINT NAME:_____

EMAIL:_____

Configuration details of the Device on which WiFI access is requested:

(only one device per student will be granted WiFi access)

Device Type: Windows Laptop / Mac Book / iPad / Android Tablet / Chrome Book

Device Make (Apple, Samsung, etc):_____

Device Model and OS:_____

MAC Address (Private Address Not Allowed):_____

(Unauthorised MAC addresses will be blocked permanently)

Appendix 6: Acceptable use of AI for pupils and staff

This appendix outlines the acceptable use of AI tools, including ChatGPT, within Lawrence Sheriff School to support teaching and learning while maintaining academic integrity and digital responsibility. ChatGPT is an AI language model developed by OpenAI and can be an educational tool in a variety of educational activities.

Compliance

- We adhere to all relevant regulations regarding data protection and privacy to ensure the safety of our pupils.
- Our use of AI tools complies with the General Data Protection Regulation (GDPR) and other applicable laws.

1. Purpose of AI use

AI tools such as ChatGPT may be used to:

- Support learning by providing explanations, summaries, and practice exercises.
- Assist in research by generating ideas, structuring information, and offering diverse perspectives.
- Enhance pupils' research, revision, writing and analytical skills.
- Aid teachers in lesson planning, resource development, and administrative tasks.
- Assist pupils in learning about AI technology and its appropriate applications.

2. Acceptable use for pupils

- AI may be used as a learning aid but must not replace independent thought and original work.
- Pupils must cite AI-generated content where applicable to ensure academic honesty.
- AI should not be used for completing assessments, coursework, or homework unless explicitly permitted by a teacher.
- Misuse of AI, such as generating inappropriate content or bypassing school policies, will result in disciplinary action.

3. Acceptable use for staff

- Staff may use AI to enhance teaching materials, generate lesson plans, and streamline administrative work.
- AI should not be used to replace professional judgment or create misleading content.
- When using AI-generated materials in assessments or resources, staff should review content for accuracy and appropriateness.

4. Responsible and ethical use

- AI should be used in a way that promotes critical thinking and responsible technology use.
- Users must be aware of AI limitations, including potential biases and inaccuracies.
- The use of AI will align with the school's safeguarding policies, data protection regulations, and overall digital safety guidelines.

5. Eligibility to use ChatGPT

- Parental consent is required for children to use ChatGPT.
- Only children who are 13 or older are eligible to use ChatGPT.
- Consent will be requested from parents as part of this our acceptable use of AI framework.

6. Data usage by ChatGPT

- Pupils will always be advised against sharing personal information with generative AI models like ChatGPT.
- Pupils do not need to create an account in order to use ChatGPT, however if they do OpenAI collects and uses the following metadata during a pupil's interactions with the service:
    - Log data
    - Usage data
    - Device information
    - Cookies
    - Analytics
    - Text input by the pupil

The details of OpenAI's complete privacy policy can be read by navigating here: https://openai.com/policies/privacy-policy

By adhering to this appendix, pupils and staff can effectively integrate AI tools while upholding the school's academic and ethical standards.