



Lawnswood School: Acceptable Use Policy (AUP) for IT and Digital Technologies

1. Purpose and Scope

This Acceptable Use Policy sets out the standards and expectations for the use of all IT and digital resources at Lawnswood School. This includes hardware, software, internet access, email services, cloud platforms, and personal devices used on site.

The policy applies to:

- All students and staff.
- Visitors and contractors using or accessing the school's IT systems.
- All school-provided and personal devices connected to the school network.

The aim of this policy is to ensure a safe, responsible, and legal use of technology in support of learning and teaching while protecting users and the integrity of our systems.

2. Core Principles

- Educational Use: All IT systems are provided primarily for educational use. Personal use must not interfere with learning, teaching, or network integrity.
- Safety and Security: The school is committed to keeping users safe online and ensuring the security of its systems.
- Accountability: All users are accountable for their use of the school's IT systems and are expected to use them in a respectful, lawful, and ethical manner.

3. Internet Use

- All internet activity is filtered through a three-tier content filter in line with UK Safer Internet Centre and Prevent duty guidelines.
- Inappropriate websites (e.g. adult content, gambling, weapons, hate speech, etc.) are blocked.

- Attempts to bypass web filtering systems (e.g. VPNs, proxies, incognito browsing) are strictly prohibited.
- Some streaming services (e.g. YouTube) are allowed for educational purposes.
- Some streaming services (e.g. Netflix, Spotify, Amazon Video/Music) are NOT allowed due to the fact they are not licensed for “public consumption”.
- Downloading software, media, or files from unapproved sources is not permitted.

4. Monitoring and Privacy

- All digital activity (internet usage, email communication, device usage, file access, printing) is monitored and logged for safeguarding, security, and educational compliance.
- Real-time, human-moderated digital monitoring solutions are used, which may collect information such as internet activity, screen captures, and user behavior.
- Monitoring is proportionate and in line with data protection laws, including the Data Protection Act 2018 and UK GDPR.
- Users should not expect any right to privacy when using school systems.
- Onsite school devices may be accessed remotely by IT staff for maintenance, support, updates, or investigations.
- Where misuse is suspected, the school reserves the right to access a user’s files, browsing history, and email accounts.

5. Plagiarism and Academic Integrity

- Submitting work copied from the internet, AI tools (see AI Policy), or another person without proper citation is considered plagiarism and will be treated as a serious academic offence.
- All assessments must reflect a student’s own understanding and effort.
- First offences may lead to redoing the work; repeated offences may result in disciplinary action, including parental involvement and potential exclusion from qualifications.

6. Game Playing and Non-Educational Use

- Use of games on school devices is prohibited unless authorised by a staff member as part of a structured lesson.
- Downloading, installing, or running any game, emulator, or unauthorised application is not permitted.
- Accessing game-related websites or forums during school hours is not allowed.
- Students may lose device access privileges if found misusing systems for entertainment purposes.

7. Email and Digital Communication

- All staff and students are provided with school email addresses for communication related to education and school business only.
- Emails must be written in a respectful and professional tone. Offensive, threatening, or inappropriate messages will not be tolerated.
- Staff and students must report any inappropriate, threatening, or suspicious emails to IT support or a safeguarding lead immediately.

8. Data Protection and Confidentiality

- Sensitive data (e.g. student records, assessment data, safeguarding notes) must only be accessed and stored on secure school-approved platforms.
- Personal USB drives are not permitted for storing school data.
- Staff and students must never share personal or confidential information over unencrypted platforms.
- Breaches of data protection, whether accidental or intentional, must be reported immediately to the School Data Protection Officer (DPO).

9. Passwords and User Accounts

- Users are responsible for maintaining the security of their accounts and must:
 - Use strong passwords.
 - Never share passwords with others.
 - Log off or lock their device when unattended.
- Any use of someone else's account or identity is strictly forbidden and may result in suspension of access or disciplinary action.

10. Equipment Use and Care

- All hardware (e.g. desktops, laptops, tablets, printers, projectors) must be treated with care and respect.
- Users must not:
 - Move or unplug equipment without permission.
 - Tamper with or attempt to repair school-owned devices.
 - Eat or drink near IT equipment.
- Printer use must be for educational use only.

- Any faults, damage or theft must be reported immediately to IT support or a member of staff.
- Deliberate damage or vandalism will be treated as a serious offence and may result in financial liability and/or exclusion.

11. Illegal and Inappropriate Activities

Use of school systems for any of the following activities is strictly prohibited:

- Creating, accessing, downloading, or distributing:
- Pornographic, racist, homophobic, or extremist content.
- Content promoting violence, terrorism, or self-harm.
- Pirated or illegal software, music, or films.
- Cyberbullying, online harassment, or doxxing.
- Hacking, phishing, or attempting to gain unauthorised access to restricted parts of the school network.
- Use of the dark web, anonymous browsers, or encryption software without explicit permission.
- Engaging in or facilitating criminal activity using school systems.

All illegal activity will be reported to the police or relevant authorities and may result in permanent exclusion.

12. Use of Personal Devices (BYOD Policy)

- Sixth Form Students and staff may use personal devices (e.g. laptops, tablets, smartphones) on the school's BYOD network.

Personal devices:

- Must not be used to bypass school systems or controls.
- Must connect only through the school's designated Wi-Fi.
- Are not permitted to store or transmit sensitive school data.
- The school reserves the right to inspect any personal device suspected of misuse on school premises.
- The school accepts no responsibility for the security, maintenance, or insurance of personal devices brought on site.

I3. Consequences of Policy Breaches

Breaches of this AUP will be dealt with in accordance with the school's Behaviour and Disciplinary Policies and may result in:

- Temporary or permanent revocation of IT access.
- Consequences in line with the school behavior policy.
- Parental involvement and formal warnings.
- Referral to external agencies including the police or local authority safeguarding teams.

I4. Student and Parent/Guardian Agreement

All students and staff agree to the AUP Agreement upon log on, confirming they understand and will comply with the policy.