Secondary Pupil Acceptable Use Agreement

V3: February 2026 onwards until revised

Pupil Acceptable Use Agreement (AUA)

Technology plays an essential role in teaching and learning at our school. To ensure that all pupils use digital tools safely, responsibly, and respectfully, the school has established a Pupil Acceptable Use Agreement (AUA).

The AUA sets out expectations for how students should use school devices, online platforms, email, internet access, and AI tools. It helps us maintain a safe and secure digital environment, protect pupils from online risks, and promote positive digital behaviour.

Students are required to follow the AUA whenever they use school IT systems. To reinforce these expectations, pupils are asked to re-accept the agreement approximately every 120 days. A prompt will appear before logging in; pupils must accept the agreement to access IT services.

For more information, please contact the school office.

1. Introduction

This IT Acceptable Use Agreement outlines the rules and guidelines for the use of the school's Information Technology (IT) resources by all pupils who attend this school. By using the school's IT resources, you agree to abide by the terms and conditions outlined in this document.

The purpose of this agreement is to ensure the responsible and ethical use of IT resources, maintain a secure computing environment, and promote positive digital citizenship among our pupils.

2. Acceptable Uses

2.1. General Usage

- You are permitted to use school-provided IT resources for educational purposes and other activities authorised by school staff.
- All use of IT resources must comply with the school's policies, procedures, and applicable laws.

- You must follow any additional rules set by your teacher for specific lessons, subjects, or platforms.

2.2. Responsible Use

- Treat all IT resources with care and respect. Do not engage in activities that could damage, disrupt, or misuse school property.
- Do not share your login credentials with anyone or attempt to access another user's account without explicit permission.
- Immediately report lost or stolen devices, suspicious activity, or accidental damage to a member of staff.

2.3. Internet Usage

- You must not use school systems, platforms or internet access to post, share or engage in behaviour that could upset, threaten, embarrass or exclude another person.
- Internet access is provided for educational purposes.
- Do not use it for illegal, unethical, or non-educational activities.
- Do not visit, download, or distribute inappropriate, offensive, or harmful content.
- Do not use proxy sites, VPNs, or other methods to bypass content filtering or monitoring.

2.4. Email Usage

- Do not use email to spread rumours, share unkind messages, pressure others, or forward content designed to embarrass or hurt someone.
- Use the school email system for school-related communication only.
- Do not send or share any messages that contain cyberbullying, harassment, any form of online abuse or violation of other school policies.
- Use clear, respectful language and appropriate tone; email is a formal record.

2.5. Data Security

- Protect sensitive information and personal data. Do not attempt to access, disclose, or manipulate data without authorisation.
- Do not introduce or spread malware, viruses, or other harmful software.
- Only store school data on approved locations (e.g., school OneDrive/SharePoint). It is best practice not to save school data on personal devices or personal cloud accounts.
- Lock your device when unattended and log off at the end of use.

2.6. Respect for Privacy

- Do not capture or share screenshots of others' work, messages or images with intent to mock or embarrass.
- Sharing altered or AI-edited images without permission is prohibited.
- Respect the privacy of others. Do not capture, share, or distribute images, videos, or personal information without consent.
- Do not attempt to access files, folders, or mailboxes that you are not authorised to view.

2.7. Social Media and Online Conduct

- You must not create or share content that targets, humiliates, or threatens others.
- Represent yourself and the school positively on social media and other online platforms.
- Do not engage in cyberbullying, harassment, or any form of online abuse.
- Do not claim to speak on behalf of the school without permission.

2.8. Network Usage

- Do not engage in excessive bandwidth usage that could disrupt the network for others.
- Do not attempt to circumvent network security or access blocked websites.
- Do not set up personal hotspots, ad-hoc networks, or connect unauthorised equipment (e.g., routers, switches, USB network adapters).

2.9. Mobile Devices and BYOD (Bring Your Own Device)

- Personal devices may be used only when authorised by staff and must connect via approved methods.
- Personal devices must not be used for bullying or harassment.
- The same rules in this Agreement apply to personal devices when used on school premises or for schoolwork.
- The school may require you to disconnect or surrender a personal device temporarily where misuse is suspected, in line with school policy and the law.

2.10. Passwords and Accounts

- Choose strong passwords, keep them secret, and change them if you believe they are compromised. You are responsible for activity carried out under your account; never tell anyone your password or use someone else's account.

2.11. Copyright, Academic Integrity and AI Declaration

- Do not plagiarise. Always credit your sources (text, images, audio, video, code).
- If you use AI or other tools to support your work, you must follow teacher instructions and, where required, declare this use.

2.12. Images, Audio/Video Recording and Publishing

- Do not record or photograph pupils or staff without permission and a valid educational reason.
- Do not post school images, recordings, names, or identifying details online without school approval.

2.13. Remote/Blended Learning and Video Conferencing

- Use only school-approved platforms. Join with your real name and school account.
- Use appropriate backgrounds, behave as you would in class, and do not record sessions unless permitted.

2.15. Monitoring, Filtering and Privacy Notice

- The school monitors and logs activity on its network, devices, email, and platforms for safety, security, safeguarding, and compliance.
- Web content is filtered. Attempts to bypass monitoring or filtering are prohibited.

16. Reporting Concerns and Safeguarding

- Report harmful or upsetting content, bullying, unsafe behaviour, suspected security issues, or device loss to staff immediately.
- If you see something wrong, say something—online safety is everyone's responsibility.

2.17. Accessibility and Assistive Technology

- You may use approved accessibility/assistive tools (e.g., read-aloud, captions, dictation) to support your learning, following teacher guidance.

2.18. Software, Licensing and Installation

- Do not install, copy, or use unlicensed or unauthorised software, apps, or browser extensions on school devices.
- Only use software provided or approved by the Trust.

2.19. Removable Media and File Sharing

- Do not use USB drives or external media unless scanned/approved; do not share files through unapproved platforms.

2.20. Physical Security

- Carry and store devices safely (e.g., in a case). Do not leave devices unattended in public areas.

3. Artificial Intelligence (AI) Usage

AI tools include any software, websites, apps, or services that use artificial intelligence to generate, analyse, or transform content (e.g., chatbots, image/audio/video generators, translation tools, code assistants).

Allowed Use

- You may use AI when approved by your teacher and when it directly supports learning.
- AI may help you understand topics, practise skills, or generate ideas, but your submitted work must remain your own.

Responsible and Safe Use

- Do not submit AI-generated work as your own. Follow teacher guidance on citing or declaring AI use.
- Do not enter personal data (yours or others') into AI tools unless a teacher explicitly permits it on an approved platform.
- Do not use AI to create inappropriate, misleading (e.g., "deepfakes"), harmful, or discriminatory content.
- Treat AI outputs critically; they may be inaccurate or biased. Check facts and use multiple sources.

Security and Access

- Do not try to bypass age gates, safety filters, or access restrictions on AI tools.
- Use only school-approved accounts and versions where provided.

Consequences

- Misuse of AI may result in academic penalties (e.g., re-submission), behaviour sanctions, and notification of parents/carers.

4. Consequences of any Violation

- Failure to comply with this IT Acceptable Use Agreement may result in disciplinary action, in line with the school Behaviour Policy.
- Sanctions may include loss of ICT access, re-doing work, device confiscation (short term), contacting parents/carers, and additional training.
- Serious or repeated breaches may be escalated in line with the Behaviour Policy and relevant laws.

5. Review and Updates

This agreement may be reviewed and updated periodically to reflect changes in technology, school policies, and legal requirements. You will be informed of any changes as they occur.

The school may issue interim notices for urgent safety or legal updates.

6. Acknowledgement

By logging onto the school IT systems, you are accepting the terms of this agreement.

Where required, pupils and parents/carers may be asked to sign to confirm they have read and understood this Agreement.