

ACCEPTABLE USE OF TECHNOLOGY (PUPILS) POLICY

Technology is integral to education at Tonbridge. It enables you to explore ideas, access knowledge from around the world, collaborate with others, express creativity, develop skills for university and beyond, and engage with subjects in ways that would be impossible without it.

Used well, technology supports curiosity, independent thinking, and genuine learning. This policy establishes expectations for the responsible, safe, and productive use of technology at Tonbridge School.

This policy applies to:

- All devices (school-owned, Pupil Device Scheme, personal) on school premises or the School network
- School accounts and cloud storage (Microsoft 365, email, OneDrive, SharePoint)
- AI tools and emerging technologies
- Online behaviour involving the school community, wherever it occurs

This Policy should be read in conjunction with the policies listed below:

- | | |
|--|---|
| • Safeguarding Policy | • Confiscations Policy |
| • Online-Safety Policy | • Privacy Notice for Boys |
| • Cyberbullying Policy | • Mobile Phone Use Policy |
| • Anti-Bullying Policy | • Taking Storing and Using Images of Pupils |
| • Behaviour Rewards and Sanctions Policy | • Guidelines for use of Email |
| • Emerging Technologies and AI Policy | • Cyber Security Policy |

FIVE CORE PRINCIPLES

Everything in this policy follows from five core principles:

1. **Use technology to support your learning, not replace it.** Technology should help you learn, create, and understand, not do the work for you.
2. **Treat others with the same respect online as you would in person.** Digital interactions have real and lasting consequences.
3. **Be honest about what is your own work.** Academic integrity means submitting work that represents your genuine understanding and effort.
4. **Understand that you have limited privacy when using school systems.** The school monitors technology use for safeguarding purposes. Don't store anything you couldn't justify to staff or parents.
5. **When in doubt, ask.** If you're unsure whether something is appropriate, speak to your teacher, tutor, or housemaster.

USING TECHNOLOGY RESPONSIBLY

Digital Responsibility

Pupils must:

- Treat others online with respect and courtesy
- Communicate constructively and professionally in digital interactions
- Use school email addresses when communicating with staff, check email regularly, and respect privacy (do not forward messages without permission)
- Report concerns about others' wellbeing or safety to a trusted adult

Academic Integrity

Pupils must:

- Submit work representing their own understanding and effort

-
- Cite sources appropriately and respect copyright. Understanding that plagiarism is presenting others' ideas or writings as your own
 - Follow subject-specific guidance on when and how technology may be used
 - Acknowledge all sources, including AI assistance where used and permitted
 - Never use indecent, obscene, offensive, or threatening language

Evaluating Information

Pupils should:

- Evaluate sources critically and recognise bias, misinformation, and unreliable content
- Understand how algorithms and platforms influence what they see
- Verify important information against multiple credible sources

ARTIFICIAL INTELLIGENCE

AI tools can support learning when used thoughtfully, but they cannot replace independent thinking or genuine engagement with material. Teachers will indicate when and how AI may be used for specific tasks. Where a teacher has given no instruction, the default position applies: AI may be used to help you understand and explore a topic, but not to produce work that you submit as your own. When in doubt, ask before using AI. The school's approach to AI is set by its AI Governance Framework and the CLEAR principles (Compliant, Literate, Ethical, Accountable, Responsible); this section sets out what that means for your day-to-day.

When AI Can Support Learning

AI may appropriately support: brainstorming ideas, researching topics, checking understanding, practising language skills, generating study materials, and creative projects where explicitly permitted by your teacher.

When Independent Work is Required

AI must not be used to:

- Generate content for submission as your own work in assessments
- Complete homework or coursework unless explicitly permitted by the subject teacher
- Bypass the development of skills that the task is designed to build
- Assist with examinations (this constitutes malpractice)

AI-Generated Images and Synthetic Media

AI can now create highly realistic images, audio, and video of people who don't exist, or depict real people doing things they never did. This creates serious ethical and legal challenges.

Strictly prohibited:

- Creating AI-generated images, audio, or video of real, identifiable people
- Creating content that could be mistaken for evidence of something someone said or did
- Sharing or amplifying synthetic media depicting real people, even if you didn't create it

Legal warning: Creating or sharing sexual or nude or semi-nude AI-generated images of anyone under 18 is a serious criminal offence under UK law, even if the image is entirely fabricated. If you encounter such content, do not share it; report it to a trusted adult immediately.

AI-generated images are not banned for appropriate uses. Creating images of fictional characters, landscapes, objects, or concepts for educational or creative work is acceptable when done transparently. Always acknowledge when AI has been used.

Critical Thinking and Independence

When using AI, pupils should:

- Verify AI outputs: AI can produce inaccurate, biased, or misleading content
- Use AI as a tool to help you think more deeply, not as a shortcut that prevents learning
- Be prepared to explain their understanding independently of AI-generated content

-
- Use school-provided AI tools (such as Copilot accessed through Microsoft 365) rather than consumer services, and must not enter personal information or schoolwork into AI tools unless they are school-approved
 - Not use personal AI accounts or paid AI subscriptions for schoolwork; Copilot, accessed through your school Microsoft 365 account, is the school's recommended and supported platform
 - Check the school's register of approved AI tools if unsure whether a tool may be used; a tool that is not on the register is not approved for schoolwork

AI is increasingly built into everyday tools such as Word, Teams and search engines, and the same expectations apply whether AI is a standalone service or a built-in feature. AI agents, meaning tools that browse, complete tasks or take actions on your behalf, must not be used with school accounts or for schoolwork unless specifically approved.

SAFETY AND SECURITY

Account Security

Keep passwords secure and confidential. Never share passwords or allow others to use your accounts. Report compromised accounts immediately to IT & Digital (via the helpdesk on the Tonbridge App) or your housemaster.

Prohibited Activities

The following are strictly prohibited:

- Using VPNs, proxy servers, mobile phone tethering, or personal data connections, or any similar systems to bypass school filtering or monitoring systems while on school premises
- Accessing, creating, or sharing illegal, pornographic, violent, discriminatory, or bullying content
- Attempting to hack systems or gain unauthorised access to accounts or files
- Installing unauthorised software on school-managed devices or deliberately introducing malware
- Downloading or distributing pirated or copyright-infringing content (music, films, software); this is illegal under UK law
- Impersonating others online or creating fake accounts in others' names
- Engaging in online gambling, financial scams, or phishing schemes
- Posting anything online that would bring the school into disrepute
- Using digital recording devices, including wearable recording devices (including glasses) while on school premises during term time without express permission of those being recorded

VPNs and circumvention tools: Using VPNs, mobile phone tethering, or similar tools undermines the school's statutory safeguarding responsibilities under Keeping Children Safe in Education. If there is a suspicion that a pupil has broken these rules, the Housemaster or System Administrator may remove the boy's device without warning, prior to an investigation taking place in conjunction with the Deputy Head Pastoral or Second Master; this investigation would include the School searching a boy's device or devices wherever suspicion arises. This approach is designed to help the School manage the risks presented by boys accessing harmful online content.

Cybercrime: Young people can become involved in cybercrime without realising the seriousness of what they are doing. Hacking, creating or sharing malware, and attacks that disrupt websites or services are criminal offences under UK law, even when framed as a joke, a dare, or a technical challenge. If you are curious about how systems and security work, speak to IT & Digital about legitimate routes to develop those skills, such as cyber security courses and competitions.

DIGITAL WELLBEING

Healthy technology use matters. Pupils should:

- Take regular breaks from screens and balance digital activities with offline pursuits
- Follow house rules on device hand-in times and avoid screens in the hour before bed
- Recognise that AI and technology cannot replace human support; seek help from tutors, housemasters, or the school counsellor for personal concerns
- Report if technology use is causing stress, anxiety, sleep problems, or affecting wellbeing

If Something Goes Wrong

If you encounter inappropriate content accidentally, close it immediately and report it to your Housemaster or a teacher—this protects you from any suggestion that access was intentional. Report cyberbullying, concerning behaviour, or safeguarding issues to Housemasters, the Deputy Head Pastoral (Designated Safeguarding Lead), the school counsellor, or external services such as Childline (0800 1111) or CEOP (www.ceop.police.uk). This includes online blackmail and financially motivated sexual extortion, where someone threatens to share real or AI-generated images unless money is paid. If this happens to you, you have done nothing to be ashamed of: do not pay, do not delete the messages, and tell a trusted adult straight away.

Filtering and Monitoring

The school is legally required to filter and monitor technology use to safeguard pupils under Keeping Children Safe in Education. These systems exist to protect you and enable staff to identify concerns early.

What the systems do:

- Filter web content and apply time-based restrictions (some social media platforms are blocked during certain hours to support focus and wellbeing)
- Monitor for safeguarding concerns such as bullying, self-harm, grooming, violence, or extremism
- Scan school email accounts and documents stored in OneDrive and SharePoint
- Generate alerts that are reviewed by trained safeguarding staff

What the systems do not do: They do not access files stored locally on personal devices. Alerts are reviewed with context by safeguarding staff, with a focus on early help and pastoral care, not punishment.

Classroom Management Software

Devices purchased through the Pupil Device Scheme have classroom management software that helps teachers keep pupils focused during lessons. This software is active during timetabled activities and allows staff to view screens, manage tabs and applications, and push content to pupil devices. It does not record screens, access files, and will not be used for surveillance outside lesson and prep times. Pupils can see when they are in a managed classroom session.

YOUR PRIVACY AND THE SCHOOL'S RESPONSIBILITIES

You should expect limited privacy when using school systems. This includes school-owned devices, Pupil Device Scheme devices, personal/BYOD devices connected to the school network, school email and cloud storage, and internet activity on the network.

The Second Master, Deputy Head Pastoral, Deputy DSLs, IT & Digital staff, and Housemasters have the right to access a pupil's school files or devices at any time where there is a safeguarding, behavioural, or legal concern. The School may search devices (school-owned, Pupil Device Scheme, or personal) where there is reasonable suspicion of prohibited content or policy breach.

Important: Whenever the network is used, an electronic trail is left that can subsequently be followed. Pupils may think it is easy to break rules without detection, but all network activity is logged and can be reviewed.

As a general rule: Do not store anything on school systems or devices that you would feel uncomfortable justifying to a member of staff or to your parents.

The School processes personal data in accordance with UK GDPR and the Data Protection Act 2018. Full details are provided in the Privacy Notice for Boys. Filtering and monitoring data is stored in UK and EU data centres. Pupils retain copyright and intellectual property rights in their work.

DEVICES AND RESOURCES

School-Owned Devices

Use school-owned devices only for educational purposes. Do not install unauthorised software or modify system settings. Report technical problems or damage to IT & Digital.

Pupil Device Scheme

Laptops purchased through the Pupil Device Scheme have a school-managed operating system. From September 2026, pupils joining the school will be required to sign up to the Pupil Device Scheme. The scheme provides pupils with a school-managed device, which allows the school to carry out its safeguarding responsibilities more effectively. These devices are the pupil's own property but are managed by the school. Apps and software are deployed via the Company Portal, managed by IT & Digital. All rules in this policy apply to these devices. Do not remove or bypass the managed operating system. Install software only through the Company Portal or with explicit IT & Digital approval.

Personal Devices

Personal/BYOD devices brought to school must comply with all applicable policies and rules when connected to the school network. Do not use personal devices to bypass school filtering or security. Ensure any inappropriate content is removed before bringing devices to school. Do not allow others to access your devices. Pupils are permitted a laptop (either their own or the school-managed device) and one other device, such as a mobile phone or a tablet; three or more devices are not permitted. Boys should not bring unnecessary devices to school without permission of their Housemaster.

Mobile Phones and Wearable Technology

Mobile phone use is governed by the Mobile Phone Use Policy. Smartwatches and other wearable technology with connectivity (Wi-Fi, mobile data, Bluetooth) are subject to the same rules as mobile phones.

Printers and Network Resources

Pupils should:

- Use school printers only for educational material related to legitimate academic or co-curricular activities
- Consider the necessity of printing in accordance with responsible environmental awareness
- Avoid downloading or storing unnecessarily large files
- Avoid excessive streaming of films, television, or music on the school network—this restricts others' use
- Respect age classifications for films and games

SANCTIONS

Depending on the severity of the offence, one or more of the following sanctions may be applied if a pupil is found to have broken any of the above rules:

- A formal warning
- Suspension of internet access
- Suspension of system account
- Device confiscation (phone, tablet, laptop)
- Formal School sanctions (including Headmaster's Detention)
- Temporary or permanent exclusion from the School

Where technology is used for illegal purposes, the school will report the matter to the police.

The school's primary approach is educational rather than punitive, and where appropriate, sanctions may be combined with support for developing better digital habits.

GETTING HELP AND IMPLEMENTATION

If you are unsure about whether something is appropriate or need guidance on technology use, speak to your teacher, tutor, or housemaster. The School is here to support you in developing responsible digital habits.

This policy is communicated through assemblies, house meetings, tutor time, and the Pastoral Education curriculum. It is published on the Tonbridge App and the school website. All staff share responsibility for supporting pupils' responsible use of technology.

Oversight: Director of IT & Digital, Second Master, and Deputy Head Pastoral (Designated Safeguarding Lead). This policy is reviewed annually or sooner if required by legislation or safeguarding guidance. Feedback from pupils (via the Tonbridge Digital Wellbeing Council), parents, and staff informs ongoing development.