



ICT Acceptable Use Policy

REVIEW DATE: July 2026

LATEST REVIEW DUE: July 2027

STAFF RESPONSIBLE: Mr Gareth Green (Assistant Head Academic)

CHAIR OF GOVERNORS: Mark Taylor

This policy should be read in conjunction with the following St Michael's policies:

- *Safeguarding Policy*
- *Staff Handbook*
- *Data Protection Policy*
- *Privacy Policy*

Introduction

This policy outlines the acceptable use of Information and Communication Technologies (ICT) at St. Michael's School. It is a living document and is reviewed regularly to adapt to new technologies and challenges. A copy of this document can be accessed on the school website. At St. Michael's, we prioritise the safety and responsible use of information technology to ensure a secure, respectful, and productive environment for our entire community.

ICT is an integral part of the curriculum across all key stages.

- **EYFS & Pre Prep:** Pupils work towards Early Learning Goals in technology through play-based experiences and distinct lessons. By the end of Key Stage 1, pupils are taught basic programming, logical reasoning, and how to communicate safely and respectfully online. Digital safety is discussed at the start of each academic year, and teachers use age-appropriate methods to reinforce these concepts.
- **Juniors & Senior School (Y3 to Shell):** Students build comprehensive digital literacy. This policy covers general ICT use as well as our 1:1 school device program (Chromebooks and iPads). At the start of each academic year (or upon mid-year entry), Form teachers review the combined Acceptable Use Pledge with their students.

Monitoring and Filtering

All school ICT infrastructure, internet access, and school-managed devices are filtered and monitored.

- **Alert System:** If our filtering system detects attempts to access websites or materials presenting a risk of harm (including, but not limited to, intolerance, racism, extremism, or self-harm), an automatic alert is generated via the **Lightspeed** filtering system and sent directly to the school's Designated Safeguarding Lead (DSL) and the IT department.
- **Reporting:** Incidents of serious misuse by staff or pupils will be reported directly to the Headteacher, and a log is maintained on file. Reports may be shared with external safeguarding services where appropriate.



Communication with Parents & Behaviour

Parents will be contacted directly if concerns arise regarding a pupil's improper use of the internet or school equipment. All digital misuse will be handled under the school's **Behaviour Policy**. Depending on the severity of the misuse, sanctions may include a temporary or permanent ban from school systems, loss of device privileges, or further disciplinary measures (up to and including exclusion).

Damage to School-Provided & 1:1 Devices

- **Ownership & Insurance:** Under our procurement program, students own their Chromebooks from the beginning of Year 5. These devices are covered by a 5-year extended warranty and accidental damage insurance, limited to **one repair per year**.
- **Reporting Damage:** If a device is damaged during school hours, it must be reported to the IT department immediately. The IT department will arrange for repair or replacement (which can take up to two weeks) and will issue a temporary loan device.
- **Loan Devices & Negligence:** If a student damages a loan device, the IT team will assess the damage and complete an incident report. If the damage is deemed to have been preventable or due to negligence, the repair or replacement costs will be passed onto the parents via end-of-term fees.
- **Damage Outside School:** If a student-owned Chromebook is damaged at home or during holidays, parents must notify the school before the student returns. School-owned iPads follow the same tracking and charging procedures.

Guidelines for Staff

- **Primary Purpose & Conduct:** School computer equipment, networks, and services are work tools provided for professional duties only. Staff must not use school devices to conduct personal business for financial gain, nor store inappropriate media. All electronic communication within the school community must remain strictly professional and utilize internal school systems.
- **Password Security:** Staff must maintain secure, complex passwords. Passwords or PINs must never be shared with colleagues or pupils, and care must be taken to prevent onlookers from seeing them.
- **Device Security & Loss:** Staff are responsible for the physical security of their assigned devices. Laptops must be stored securely when not in use, and passwords must never be written down or kept with the device. If a device is lost or stolen, it must be reported immediately to the IT department and the Police. Staff must obtain a crime reference number for insurance purposes.
- **Data Protection & Storage:** Staff must maintain reasonable care when transporting portable equipment. To comply with Data Protection laws, personal data regarding pupils (such as contact details or sensitive files) must not be stored locally on hard drives; instead, approved secure cloud systems must be used. Staff are prohibited from taking copies of school personal data when they leave the employment of the school.
- **Software and AI Tools:** All software and online learning platforms must be vetted and installed by the IT department to ensure licensing compliance. Staff are encouraged to use approved generative AI tools (such as **Google Gemini** and **NotebookLM**) to enhance teaching, planning, and administrative efficiency. Staff must vet all AI-generated outputs for accuracy and ethical alignment before use.



- **Network Audits:** The IT department reserves the right to maintain software and file audits. Network administrators can access user files only when explicitly authorized by the Headteacher, Chair of Governors, or Office Manager. The school retains the right to reclaim any school-owned device at any time without explanation.

Artificial Intelligence (AI) - Student Framework

St. Michael's School prepares students for a digital future by teaching the responsible, ethical, and critical use of Artificial Intelligence. To protect academic integrity, **all work submitted must be demonstrably the student's own.**

We utilise a **Traffic Light System** across all learning environments to clearly communicate permissions for any given task:

- **Red Light:** No AI use permitted. Work must be entirely independent to assess your own knowledge.
- **Amber Light:** AI may be used for support (e.g., brainstorming, spell checking, or clarifying ideas), but the final writing must be your own.
- **Green Light:** AI can be fully utilised as a tool for the task, provided proper attribution and referencing are included.

Progression by Year Group:

- **Years 3 and 4:** Students are introduced to supervised, integrated AI features within approved creative applications (like Canva or Adobe Express) strictly under teacher direction.
- **Years 5 to 8:** Students are formally taught how to prompt and interact safely with AI assistants like **Google Gemini**, focusing on digital literacy, ethical boundaries, and the Traffic Light System.
- **Shell (Year 9):** Students engage in advanced critical appraisal of AI models. They learn to evaluate AI for bias, data privacy, and reliability, using AI as a support for (rather than a replacement of) critical thought.



Appendix A:

My Digital Citizenship & Device Pledge (Years 3 to Shell)

Note for Form Rooms: *This combined agreement applies to all school computers, ICT equipment, iPads, Chromebooks, and personal devices used in school or online at home.*

1. Look After My Technology

- I will treat all school equipment with care and respect.
- I will keep my Chromebook or iPad safe in my bag so it does not get wet, crushed, or dropped.
- I will keep food, snacks, and drinks far away from devices to avoid messy spills.
- If something breaks or stops working, I will tell a teacher or the IT team straight away. I will not try to fix it myself.

2. Be Ready to Learn

- I will bring my device to school every single day.
- I will make sure my device is **fully charged (100%)** every morning before school starts.
- When using shared school equipment, I will leave it tidy and plug it back into the charger for the next person.
- I will only use my device for schoolwork, using the apps and websites my teacher has said are okay.

3. Keep Things Private and Secure

- I will only log in using my own username and password.
- I will keep my passwords a secret and never share them with friends.
- I will never let anyone else use my personal device or my school account.
- I will not give out personal information online (like my phone number, home address, or photos) without a teacher's permission.

4. Think of Others (Be Kind Online)

- I will always use polite, kind language. I will never use school technology to bully, hurt, or upset anyone.
- I will always ask for permission before taking a photo or recording a video of another person.
- If I see something online that makes me feel uncomfortable, scared, or upset, I will close my screen or email and tell a teacher immediately.

5. Be Honest (My Work and AI)

- I will always show academic honesty. The work I turn in must be my own creation, not copied from the internet or a classmate.
- I will look at the **AI Traffic Light** in my classroom before starting a task:
 - **Red:** No AI allowed at all.
 - **Amber:** I can use AI to help brainstorm or proofread, but I must write the work myself.
 - **Green:** I can use AI to help complete the project, but I must explain how I used it.



- I will never use tools like Google Gemini to do my work *for* me and pretend I wrote it. That is cheating.

6. Remember: Nothing is Invisible

- I know that the school filters and monitors what I do on school devices and networks to keep me safe. I have no expectation of privacy when using school systems.
- I understand that the school cares about my well-being. If I am involved in unkind or inappropriate messages on social media outside of school hours, the school will investigate to protect its pupils.

The School Device Tracker & Consequences

To help me build great habits, the school uses a **Device Tracker**. If I do not bring my device to school, forget to charge it, or misuse it, it will be recorded on the tracker.

- **3 Incidents in one academic year** = A formal warning and a conversation with my teacher and parents.
- The tracker resets to zero at the start of every academic year.
- Serious or continuous breaking of these rules may mean I lose my device privileges or face school sanctions.

I have read this pledge (or had it explained to me). I understand these rules and agree to follow them to keep myself and our school community safe.

Signed