IT ACCEPTABLE USE, DIGITAL SAFETY AND ARTIFICIAL INTELLIGENCE POLICY

This policy applies to all members of the St Columba's College community, including students, staff, parents, carers, visitors and any other users of College systems. It covers all use of technology associated with the College, whether on-site or off-site, and applies to College devices, networks and systems, as well as personal devices where their use impacts the College environment.

Education at St Columba's College is conducted in the tradition of the Brothers of the Sacred Heart. The College seeks to provide a safe and supportive environment in which all individuals can flourish. This extends to the digital environment, where technology must be used in a way that reflects the College's values of Known, Valued and Treasured.

Policy owner:	Bursar
Date reviewed:	June 2026
Date of next review:	June 2027
Ratify by governors:	Yes

A member of the HMC & IAPS. St Columba's College and Preparatory School is a Company limited by guarantee.
Registered as above. Registered Company No: 4228443 Charity No: 1088480 VAT No: 479 9962 95

Contents

1. Application, Purpose and Scope 3
2. Safeguarding, Filtering and Monitoring 3
3. Online Safety and Digital Conduct 4
4. Artificial Intelligence 4
4.1 Principles of Use 5
4.2 Age Restrictions and Access 5
4.3 Use in Teaching and Learning (Students) 5
4.4 Academic Integrity and Malpractice 5
4.5 Transparency and Referencing 6
4.6 Accuracy, Bias and Misinformation 6
4.7 Data Protection, Privacy and Intellectual Property 6
4.8 Staff Use of AI 6
4.9 Safeguarding Risks Associated with AI 7
4.10 AI-Enabled Devices, Wearables and Covert Recording 7
5. Devices, Systems and Security 8
6. Mobile Phones and Wearable Devices 9
7. Communication and Use of College Platforms 9
8. Examinations and Controlled Conditions 10
9. Sanctions 10
10. Review 10
Appendix: Glossary 11

1. Application, Purpose and Scope

Digital technologies, including artificial intelligence, are now integral to education and daily life at St Columba's College. They provide significant opportunities to enhance teaching and learning, but also present risks relating to safeguarding, data protection, academic integrity and wellbeing. This policy sets out how those risks are managed and the expectations placed on all users.

This policy should be read in conjunction with the Safeguarding Policy, Prevent Policy, Mobile Phone Policy, Cyber Security Policy, Behaviour Policy, Staff Code of Conduct, E-Safety for Students Policy, Data Protection policies and statutory guidance including Keeping Children Safe in Education (KCSIE).

2. Safeguarding, Filtering and Monitoring

The College has a statutory duty to safeguard and promote the welfare of children, including online. In line with national guidance, the College uses automated filtering and monitoring systems (including content, keyword, and behavioural monitoring) across networks and College devices. Logs are retained in accordance with the College Data Retention Policy and Data Protection legislation and accessed only by authorised staff where appropriate and proportionate.

All use of College technology may be subject to filtering, monitoring and logging. Any misuse may be recorded and investigated in line with College safeguarding, disciplinary and data protection procedures.

These systems operate across the College network and on College-issued devices, both on-site and off-site. They are designed to reduce risk but cannot eliminate it entirely. The College recognises that unauthorised and unsupervised use of technology, including AI, may occur and has systems in place to identify and respond to such use. All users must therefore act responsibly and remain vigilant.

The College applies appropriate filtering and monitoring systems to its IT networks and devices in order to support safeguarding duties. Monitoring is routinely undertaken during the College working day and reasonable, proportionate attempts are made to apply monitoring outside these hours where technically feasible. However, where College-issued devices are used outside normal College hours, including evenings, weekends and holiday periods, responsibility for the supervision and appropriate use of the device rests with parents and carers, in line with their responsibility for other technology available within the home. The College cannot reasonably supervise or control all use of devices outside normal College hours or beyond its direct oversight. Parents and carers are expected to support safe, responsible and lawful use of technology and to work in partnership with the College in promoting online safety.

The College recognises that emerging technologies, including AI, increase both the scale and sophistication of potential risks. These include the creation of realistic but false communications, impersonation, generation or sharing of nude or semi-nude images,

A member of the HMC & IAPS. St Columba's College and Preparatory School is a Company limited by guarantee.
Registered as above. Registered Company No: 4228443 Charity No: 1088480 VAT No: 479 9962 95

and the creation of harmful or misleading content. The College's safeguarding approach reflects these risks.

Any concerns relating to online safety, including those involving AI, must be reported immediately to a member of staff. Staff must follow safeguarding procedures, reporting immediately to the Designated Safeguarding Lead (DSL) via CPOMS where appropriate. The DSLs will conduct an initial triage and, if appropriate, involve the Deputy Head, DPO, the LADO or police; outcomes and actions will be recorded on CPOMS. Where concerns involve personal data or devices, the Bursar as the College's Data Protection Officer (DPO) must also be informed. Where necessary and proportionate, the College reserves the right to access user accounts, files, emails, cloud storage and digital activity for safeguarding, security, operational or investigative purposes. Such access will only take place under appropriate authorisation and in accordance with College procedures and data protection obligations.

Any attempt to bypass filtering or monitoring systems, or to undermine safeguarding controls, will be treated as a serious breach of this policy.

3. Online Safety and Digital Conduct

All users are expected to use technology in a safe, respectful and lawful manner. This applies to communication, content creation and all interactions within the digital environment.

Users must not access, create, store or share content that is harmful, offensive, abusive or illegal. This includes material that is discriminatory, exploitative or designed to mislead. The creation or distribution of manipulated content, including that generated or altered through AI, is not permitted where it may cause harm or misrepresent others. Users must not engage in cyberbullying, harassment or intimidation, and must not share images, recordings or personal information without appropriate consent. Users should recognise that content shared online or generated digitally may be copied, distributed or retained beyond their control and may cause lasting harm.

Students are expected to report any concerns immediately. Students are also taught how to keep themselves safe online through the College's pastoral and digital literacy curriculum. Staff must act on concerns in accordance with safeguarding procedures. Parents and carers are expected to support the College by reinforcing these expectations at home, engaging with College communications and guidance relating to online safety, and raising any concerns promptly.

4. Artificial Intelligence

The College recognises that AI, including generative AI, is an increasingly significant part of education and wider society. Its use must be carefully managed to ensure that it supports learning while maintaining safeguarding, ethical standards and academic integrity. This policy reflects national guidance, including the Department for Education's guidance on the safe and effective use of generative AI in education, and the expectations set out in Keeping Children Safe in Education.

AI includes generative tools such as ChatGPT, Microsoft Copilot, Claude and Google Gemini, as well as AI embedded within digital platforms used by the College, for example Seneca Learning.

4.1 Principles of Use

The default position across the College is that students do not use generative AI in their work unless explicitly permitted by a member of staff, for students in Form 3 and above only. Where AI is used, it must be for a clearly defined educational purpose and must support, rather than replace, independent thinking and learning. All work produced with the support of AI remains the responsibility of the individual and should not be released without detailed human oversight. This applies equally to students and staff.

4.2 Age Restrictions and Access

In line with industry standards and platform requirements, generative AI tools are not to be used by students under the age of 13. Within the College, access to generative AI is introduced in a structured and progressive way. Students below Form 3 will not be expected to use generative AI independently, and any exposure will be through teacher-led demonstration or supervised activity. From Form 3 onwards, students may be introduced to AI tools in a controlled and supported manner. At all stages, use must comply with both platform age restrictions and College expectations. The College will support students in developing AI and digital literacy, including understanding how AI works, its limitations, ethical considerations, misinformation, bias and critical evaluation of AI-generated content.

4.3 Use in Teaching and Learning (Students)

Where AI use is permitted by a teacher, expectations will be clearly defined. The College adopts a structured approach to classroom use, which follows this framework:

Red – AI use is not permitted. This applies to assessments, examinations and tasks designed to assess independent understanding.
Yellow – AI use is limited. AI may be used to support planning, organisation or idea generation, but all submitted work must be written by the student. Outputs must be checked carefully.
Green – AI use is permitted. AI may be used more freely to support learning, provided outputs are critically evaluated and appropriately referenced.

Unless a teacher explicitly states otherwise, AI use should be assumed to be prohibited. The use of AI and digital technologies may also form part of reasonable adjustments or support arrangements for students with additional needs/EHCPs/individual plans. Any such use must remain appropriate, proportionate and supported by suitable safeguards and documented where appropriate within individual support arrangements.

4.4 Academic Integrity and Malpractice

All users must maintain the highest standards of academic integrity. Students must not submit work generated by AI as their own, nor reproduce AI-generated responses in assessed work. Any such use constitutes malpractice.

In line with examination regulations, all work submitted must be the candidate's own. Students may be required to demonstrate their understanding of submitted work. The misuse of AI in assessments will result in referral to awarding bodies/JCQ, which may result in disqualification, and further disciplinary action. Any suspected misuse of AI will be investigated. Steps include:

1. initial review by subject teacher;
2. interview with pupil to establish understanding and authorship;
3. consideration by Head of Department and DSL if safeguarding concerns arise;
4. proportionate sanctions in line with Behaviour Policy.

Students will be given the opportunity to demonstrate their knowledge under controlled conditions where appropriate. The College may use a range of methods to investigate suspected malpractice, including professional judgement and technological tools, although no automated detection system should be relied upon in isolation.

4.5 Transparency and Referencing

Where AI is used appropriately, its use must be transparent. Users must clearly indicate the AI platform used, the purpose of its use, the nature of the input or prompt and how the output has been used or adapted. This applies to both students and staff. Transparency is essential to maintain academic integrity and trust.

4.6 Accuracy, Bias and Misinformation

AI-generated content may be inaccurate, biased, incomplete or misleading. All users must exercise critical judgement and must not rely on AI outputs without verification. Staff must ensure that any AI-generated content used in teaching is accurate, appropriate and suitable for the students' context. Students must be taught to evaluate AI outputs critically. Users should also be mindful of the environmental impact associated with excessive or unnecessary use of AI technologies and ensure that their use is proportionate and purposeful.

4.7 Data Protection, Privacy and Intellectual Property

The use of AI must comply with data protection legislation and intellectual property law. Users must not input personal, sensitive or identifiable data into AI tools. This includes information relating to students, staff or families.

The College does not permit student work or other protected material to be used to train AI systems without appropriate permission. Users must be aware that AI-generated outputs may infringe copyright, intellectual property or licensing rights.

4.8 Staff Use of AI

Staff may use AI to support planning, resource creation and administrative tasks. However, all outputs must be critically reviewed for accuracy, bias and suitability before use. AI must not replace professional judgement. The quality and appropriateness of all materials remain the responsibility of the member of staff.

AI may be used to support feedback, but final judgements must be made by the teacher. AI must not be used to mark summative assessments or any work contributing to formal data collection. In report writing, AI may support drafting or structure, but all reports must reflect the teacher's own knowledge and understanding of the student.

Staff must ensure that any use of AI is transparent and complies with safeguarding and data protection requirements. Staff should exercise particular caution when using AI live in lessons or demonstrations, especially where prompts may generate unpredictable, controversial or inappropriate outputs. Staff will receive appropriate training and updates relating to AI, safeguarding, data protection and effective educational use as technologies and guidance evolve.

4.9 Safeguarding Risks Associated with AI

AI can be used to generate realistic but false communications, impersonate individuals, or produce harmful or inappropriate material. These risks are taken seriously. Any use of AI to deceive, harm or mislead others will be treated as a safeguarding concern. This includes, but is not limited to, the creation of fake emails, messages or images designed to imitate others.

4.10 AI-Enabled Devices, Wearables and Covert Recording

Devices capable of recording, transmitting or generating content, including AI-enabled wearables, present significant safeguarding and data protection risks. For the purposes of this policy, wearable devices include, but are not limited to, smart watches, smart glasses, earbuds, neural bands, smart pens and any device capable of capturing, storing or transmitting audio, video or text, particularly where such functions may not be immediately visible.

The use of such devices is not permitted on site or during College-related activities unless explicitly authorised for a clearly defined educational or medical purpose. Wearable devices that enable communication, internet access, recording or AI-assisted functions are treated in the same way as mobile phones and are subject to the same restrictions set out in this policy. Devices used solely for approved health or medical monitoring purposes, for example diabetic blood glucose monitoring, may be permitted in line with individual care plans, provided they are not used for additional communication, recording or internet-enabled functions.

The use of any recording device is strictly prohibited in areas where privacy is expected, including toilets, changing rooms, medical spaces and residential settings on trips. Any use of wearable devices for recording, whether overt or covert, must be clearly authorised in advance and communicated to those affected.

Where a device is suspected of being used for covert recording or unauthorised transmission, it must be secured where safe to do so and reported immediately to the Designated Safeguarding Lead (DSL) and Data Protection Officer (DPO). Such incidents will be treated as both safeguarding and data protection concerns and managed in accordance with College procedures.

Staff must ensure that wearable devices do not enable communication, recording or notification use during teaching or contact time. Wearable devices are not permitted within EYFS environments. Parents, carers and visitors are also expected to comply with these expectations when on-site or attending College events.

5. **Devices, Systems and Security**

College devices and systems are provided for educational use and must be treated with care. Users must not interfere with device settings, install unauthorised software, or attempt to bypass security controls. Devices must be used in accordance with staff guidance. The College uses approved digital platforms (for example Microsoft-based systems), to support learning and communication. Users should not sign up to or use unauthorised software or cloud platforms. These must be used appropriately and in line with College expectations. Cyber security risks are taken seriously. Users must not engage in any behaviour that could compromise the security of College systems, including sharing passwords, accessing unauthorised systems or responding to suspicious communications.

The College will seek to ensure that digital platforms, including AI-enabled technologies, are procured and implemented in line with safeguarding, data protection and educational best practice. Consideration will include data minimisation, transparency of AI models and processing, vendor accountability, the ability to remove or delete data where appropriate, and evidence of educational benefit and impact.

Users must not attempt to bypass, disable or interfere with filtering, monitoring or security systems, including through the use of VPNs, proxy services, unauthorised software or other methods intended to evade College safeguards. Unauthorised access to systems, accounts, data or networks is strictly prohibited. Users must not attempt to monitor network traffic, probe, scan or test the vulnerability of systems or services without explicit authorisation from the College. Any deliberate attempt to disrupt, degrade or deny access to College systems or services will be treated as a serious breach of this policy.

Users should avoid the use of portable storage devices wherever possible and instead use College-approved cloud storage systems. Where portable storage devices are used, this must be in accordance with College guidance and appropriate security precautions. Users must not knowingly introduce viruses, malware or other harmful software to College systems or networks. Users are responsible for maintaining the security and confidentiality of their accounts and passwords and must not share login credentials or allow others to access systems using their accounts. Users must ensure that devices are locked or logged out when left unattended.

Users must not engage in illegal downloads, use of unlicensed images or music in any work, screen recording of licensed video content.

6. **Mobile Phones and Wearable Devices**
The use of mobile phones is strictly controlled and should also be read in conjunction with the College's Mobile Phone Policy.

Prep students are not permitted to use mobile phones during the school day. Any phones brought to school must be handed into Reception at the start of the day and collected at the end.

Students in KS3 and KS4 are required to place mobile phones and any wearable devices (see Section 4.10) in secure pouches at the start of the school day under staff supervision. Phones must remain secured for the duration of the day and may only be accessed with permission in designated locations such as Reception.

Sixth Form students may use mobile phones in the ground floor of the Xavier centre only, but not in lessons or general school spaces unless specifically authorised by a member of the SLT to do so.

Wearable devices (see 4.10) that enable communication, internet access or recording are treated in the same way as mobile phones and are subject to the same restrictions. Devices used solely for health monitoring may be permitted in line with individual care plans.

Separate expectations regarding the use of mobile phones and wearable devices may apply during educational visits and residential trips and will be communicated where appropriate.

Staff, visitors and other adults on site are expected to use mobile phones and wearable devices responsibly and appropriately, particularly where students are present or where safeguarding and privacy considerations apply. Staff should restrict personal mobile phone use to private offices, staffrooms or other designated areas wherever possible. Visitors are not permitted to use their mobile phones or wearables in any parts of the school where there are students present.

7. **Communication and Use of College Platforms**
All communication conducted through College systems must be appropriate, respectful and relevant. Users must not contact staff through personal accounts or engage in inappropriate or excessive messaging. Platforms provided by the College must be used in accordance with their intended purpose. This will and can be monitored through the College's filtering and monitoring processes.

Parents and carers should expect that official communication from the College will be conducted through recognised and authorised channels.

A member of the HMC & IAPS. St Columba's College and Preparatory School is a Company limited by guarantee.
Registered as above. Registered Company No: 4228443 Charity No: 1088480 VAT No: 479 9962 95

8. **Examinations and Controlled Conditions**
Strict rules apply to the use of technology in examinations and controlled conditions. No device capable of communication, storage or recording may be brought into an examination unless explicitly authorised as part of an access arrangement. The use of AI or any unauthorised technology in assessments constitutes malpractice. This will result in referral to the relevant awarding body or JCQ, who will determine any further action, which may include disqualification.

Prior to formal examinations, candidates are briefed on banned devices and asked to sign a declaration that work is their own. Examination rooms will be checked for unauthorised devices; any suspected use of AI during exams will be investigated and reported to awarding bodies per JCQ/awarding body regulations.

9. **Sanctions**
Breaches of this policy will be addressed in accordance with the relevant College procedures.

Sanctions may include:
- confiscation of devices
- restriction of access to systems
- disciplinary action

Serious breaches, particularly those involving safeguarding concerns or misuse of AI, may result in more significant consequences. Sanctions will be proportionate and may be accompanied by restorative education (e.g., further digital literacy training) where appropriate. Serious breaches involving safeguarding will follow safeguarding procedures and may prompt exclusion.

10. **Review**
Oversight of this policy involves the College Leadership Team, Designated Safeguarding Leads, IT Services, Data Protection Officer and other relevant staff responsible for safeguarding, digital systems and operational implementation. This policy will be reviewed annually, or sooner where required, in response to changes in legislation, safeguarding guidance or developments in technology.

Appendix: Glossary

Artificial Intelligence (AI): Technology enabling systems to process information and generate outputs.

Generative AI: AI capable of producing content such as text, images or audio.

AI-embedded systems: Platforms that use AI to adapt responses or personalise learning.

Covert recording: Recording without knowledge or consent.

Wearable devices: Devices worn on the body with digital capabilities.