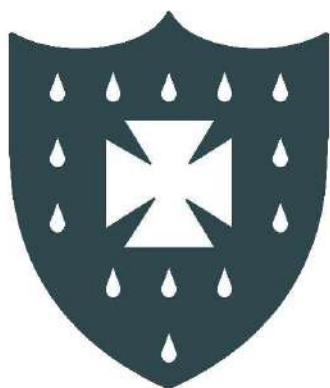




S. Anselm's Prep School Peak District

Policy Title: **Online Safety, Technology & AI Policy**

Policy Category: **Pastoral**

Policy Number: P10

Policy Owner / Author:	Alison Whawell
Approved by:	Head
Date Approved:	August 2026
Next Review Date:	August 2027
Version:	1.0
Appendices:	• Appendix 1: Staff Acceptable Use Agreement • Appendix 2: Pupil Acceptable Use Agreement • Appendix 3: Personal Device (iPad/Laptop) Acceptable Use Agreement
Related Policies:	- o Anti-bullying Policy - o Behaviour Management Policy - o Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE) - o Data security and GDPR - o Safeguarding and Child Protection Policy - o Searching, Screening and Confiscation Policy - o Staff Code of Conduct - o Image use, mobile phone and social media procedures (Staff Handbook)
Confidentiality Label:	☐ Internal Use Only ☐ Parent Web Page ☐ Public Document
Contact for Queries:	Alison Whawell

✦ This document is controlled and reviewed as part of the School's policy management process. Please refer to the school's website or Teams to ensure you are using the most up-to-date version.

1. Purpose and Aims

S. Anselm's School recognises that technology and artificial intelligence can enrich teaching, learning, communication and administration. Their use must be safe, lawful, ethical, age-appropriate and subject to effective human oversight.

This policy aims to:

- safeguard pupils, staff and the wider school community when using technology;
- set clear expectations for the safe and responsible use of school and personal devices;
- promote critical, ethical and transparent use of artificial intelligence;
- protect personal, sensitive and confidential information;
- ensure appropriate filtering, monitoring and cybersecurity arrangements;
- educate pupils to recognise, manage and report online risks; and
- provide clear procedures for responding to online safety and AI-related concerns.

Online safety is an integral part of the school's safeguarding arrangements and is considered through four broad areas of risk:

Content: exposure to illegal, inappropriate, harmful, false or misleading material, including misinformation and AI-generated content.

Contact: harmful interaction with other people or generative AI applications, including grooming, exploitation, impersonation and inappropriate chatbot interactions.

Conduct: behaviour that causes or increases the likelihood of harm, including cyberbullying and the creation or sharing of manipulated, explicit or AI-generated imagery.

Commerce: gambling, phishing, inappropriate advertising, fraud, scams and financial exploitation.

2. Scope

This policy applies to:

- all pupils, including those in EYFS and boarding;
- all staff, Governors, volunteers, visitors, contractors and peripatetic staff;
- parents and carers when accessing school systems or attending school activities;
- school-owned and personally owned devices used in connection with school;
- internet access, email, Microsoft Teams, learning platforms, social media, cloud services and artificial intelligence tools; and
- online behaviour taking place outside school where it affects the welfare of pupils, members of the school community or the safe operation and reputation of the school.

This policy should be read alongside the related documents listed in the policy information table.

All staff and pupils must read and comply with the Acceptable Use Agreement appropriate to their role. Pupils who are authorised to bring a personal iPad or laptop into school must also comply with the Personal Device Acceptable Use Agreement. See Appendices 1, 2 and 3.

3. Artificial Intelligence

3.1 Principles

The school's approach to AI is guided by the following principles:

1. AI supports human thinking, teaching and learning; it does not replace professional judgement, teacher expertise or pupil effort.
2. AI use must be safe, lawful, ethical, transparent and appropriate to the user's age and the educational purpose.
3. Users remain accountable for all work, decisions and communications produced with AI assistance.
4. AI-generated outputs must be checked for accuracy, bias, misinformation, inappropriate content and infringement of intellectual property.
5. Personal, sensitive, safeguarding or confidential information must not be entered into an unapproved AI tool.
6. The use of AI must respect academic honesty. AI-generated or AI-assisted work must not be presented as wholly the user's own.
7. Significant decisions about pupils, staff, admissions, assessment, safeguarding, complaints or disciplinary matters must always be made by an authorised person and not delegated to AI.

3.2 Approved AI tools

Staff and pupils may use only AI tools approved by the school and Addooco through the appropriate IT, safeguarding and data-protection processes.

Microsoft Copilot within the school's approved Microsoft environment is the school's preferred generative AI platform for staff use. Approval does not remove the user's responsibility to protect information, verify outputs and exercise professional judgement.

Unapproved public AI platforms must not be used for school business or with pupil information. Before a new AI application is introduced, the school will consider age restrictions, safeguarding, data use, data protection, filtering and monitoring, accuracy, bias, accessibility, intellectual property and educational value.

3.3 Staff use of AI

Staff may use approved AI tools to assist with lesson preparation, routine communications, ideas and discussion prompts, summaries of non-confidential information, training and administrative materials, translation subject to checking, and feedback on non-summative work.

Staff must:

- review, adapt and take responsibility for every AI-assisted output;
- check outputs for accuracy, bias, fabricated references and unsuitable content;
- disclose material AI use where transparency is appropriate;
- use school accounts and approved systems;
- respect copyright and intellectual property;
- ensure AI use does not diminish teaching quality, professional judgement or relationships with pupils; and
- report unsafe, harmful or unexpected output.
- comply with the Staff Acceptable Use Agreement in Appendix 1 when accessing or using AI and other school technology.

Staff must not use AI to:

- make final decisions about admissions, safeguarding, assessment, discipline, complaints, employment or pupil welfare;
- assess or provide final feedback on summative examinations or formal coursework;
- determine whether a pupil has cheated or plagiarised without wider evidence and human judgement;
- infer or assess a person's emotional condition;
- create misleading, discriminatory, degrading or harmful content;
- impersonate another person;
- process confidential, commercially sensitive, safeguarding or personal information in an unapproved AI tool; or
- send AI-generated communications without appropriate human review.

3.4 Pupil use of AI

Pupils will be taught that AI outputs can be inaccurate, biased, fabricated or misleading and must be independently checked.

All pupil use of AI must also comply with the Pupil Acceptable Use Agreement in Appendix 2 and, where a personal device is used, the Personal Device Acceptable Use Agreement in Appendix 3.

Pupils may use an approved AI tool only when directed or permitted by a teacher, for a clear educational purpose, in accordance with age restrictions and consent requirements, through a school account where provided, and with appropriate supervision.

Pupils under 13 must not independently use generative AI tools as part of school-directed activity. A teacher may demonstrate an approved AI tool without pupils operating it. Pupils aged 13 and over may use approved generative AI tools only where permitted by the tool's conditions, school arrangements and appropriate parental consent.

Pupils must not:

- enter their own or another person's personal information, photographs or confidential material into an AI tool;
- submit AI-generated work as their own;
- use AI in an assessment unless expressly permitted;
- use AI to bully, harass, intimidate, impersonate, deceive or exploit another person;
- create or distribute deepfakes, altered images, fake messages or fabricated accounts;
- use AI to create explicit, discriminatory, violent or otherwise harmful material; or
- attempt to bypass school filtering, monitoring or security controls.

AI-generated or AI-assisted work must be acknowledged in the way directed by the teacher.

3.5 AI safeguarding risks

The school recognises that AI may be used to create deepfake media, alter images of children, impersonate trusted people, facilitate grooming or fraud, generate convincing misinformation, support bullying, provide unsafe advice or encourage over-reliance.

Any AI-generated or manipulated nude or semi-nude image involving a child will be treated as a safeguarding concern, whether or not a real photograph was used.

4. Roles and Responsibilities

4.1 Governors and the Head

- provide strategic oversight of online safety, technology and AI;
- ensure appropriate policies, resources and staff training are in place;
- ensure risks associated with new technology are assessed before use;
- ensure filtering and monitoring arrangements are effective;
- receive appropriate reports on significant incidents and emerging risks; and
- ensure filtering and monitoring effectiveness is formally reviewed at least once each academic year.

4.2 Designated Safeguarding Lead

The DSL, Alison Whawell, has lead responsibility for online safety as part of safeguarding and will:

- understand the school's filtering and monitoring systems;
- provide advice on online and AI-related safeguarding concerns;
- ensure concerns are recorded, assessed and escalated appropriately;
- identify patterns, vulnerable pupils and emerging risks;
- ensure staff receive appropriate online safety and AI safeguarding training;
- work with the Head, IT support, Addooco and external agencies as required; and
- provide information and guidance to pupils, staff, parents and Governors.

Overall responsibility remains with the DSL even where activities are delegated to a trained deputy.

4.3 Staff

- follow this policy and follow this policy and the Staff Acceptable Use Agreement in Appendix 1;

- model safe, respectful and responsible technology use;
- protect passwords, devices and information;
- use only approved platforms, applications and AI tools;
- provide appropriate supervision when pupils use technology;
- teach pupils to question and verify online and AI-generated content;
- recognise that pupils with SEND or other vulnerabilities may face additional online risks;
- report concerns to the DSL or a deputy without delay; and
- preserve potential evidence and not conduct their own safeguarding investigation.

4.4 IT support

- maintain appropriate cybersecurity, access controls, filtering and monitoring;
- support the DSL and leadership team with reports and technical advice;
- ensure approved changes are logged;
- investigate technical concerns when authorised;
- support the annual review of filtering and monitoring; and
- assess new systems and AI tools through the appropriate approval and Data Protection Impact Assessment (DPIA) processes.
- support the implementation of the Staff, Pupil and Personal Device Acceptable Use Agreements in Appendices 1, 2 and 3, including the approval and checking of personal devices where required.

4.5 Pupils

- follow the Pupil Acceptable Use Agreement in Appendix 2 and, where authorised to use a personal device, the Personal Device Acceptable Use Agreement in Appendix 3;
- keep passwords secure;
- use technology only for authorised purposes;
- communicate respectfully;
- protect personal information;
- follow teacher instructions when using AI;
- check information before accepting or sharing it;
- acknowledge AI assistance when required; and
- tell a trusted adult if something worries them online.

4.6 Parents and carers

- reinforce safe, respectful and age-appropriate technology use;
- understand the benefits and risks of AI;
- support the school's device, mobile phone and acceptable-use arrangements;
- monitor changes in behaviour that may indicate online harm;
- report relevant concerns promptly; and
- avoid sharing images or information about other children without permission.
- read and support their child's compliance with the Pupil Acceptable Use Agreement in Appendix 2 and, where applicable, sign and support the Personal Device Acceptable Use Agreement in Appendix 3;

5. Education and Training

Online safety and AI literacy will be embedded across computing, PSHE and other relevant curriculum areas. Pupils will receive age-appropriate education about:

- the four areas of online risk;
- privacy, passwords and digital footprints;
- cyberbullying, grooming, exploitation and scams;
- misinformation, disinformation and deepfakes;
- how generative AI works and its limitations;

- bias, hallucination and verification of AI outputs;
- copyright, plagiarism and academic honesty;
- safe prompting and protection of personal information;
- reporting, blocking and seeking help; and
- respectful and ethical use of technology.

The Pupil Acceptable Use Agreement in Appendix 2 will be explained in an age-appropriate way and revisited regularly. Pupils using authorised personal devices will also be supported to understand the additional expectations in Appendix 3.

Staff will receive online safety training at induction, updated regularly and at least annually. Training will include filtering and monitoring responsibilities, AI-generated content, deepfakes, data protection and reporting procedures. Staff will be introduced to the Staff Acceptable Use Agreement in Appendix 1 during induction and will be required to confirm that they have read, understood and agreed to follow it. The school will provide parents with guidance on emerging online and AI risks where appropriate.

6. Filtering, Monitoring and Cybersecurity

The school will maintain age-appropriate filtering and monitoring on its networks and school-managed devices, supported by Addooco and the school's approved technical systems.

- assign clear responsibility for filtering and monitoring;
- block harmful and inappropriate content without unreasonably restricting teaching and learning;
- monitor school systems proportionately for safeguarding and security purposes;
- prioritise vulnerable pupils where appropriate;
- record and respond to identified concerns;
- inform users that school systems may be monitored;
- keep filtering, monitoring and security arrangements under continuing review; and
- complete and record a formal effectiveness review at least annually.

Filtering and monitoring do not replace appropriate supervision, professional curiosity or online safety education. Users must not bypass controls through VPNs, proxy services, browser extensions or other means.

7. Safe Use of Technology

School technology must be used safely, lawfully, respectfully and for authorised purposes. Detailed expectations for staff and pupils are set out in the Staff and Pupil Acceptable Use Agreements in Appendices 1 and 2.

Users must:

- use their own account and keep passwords private;
- lock or log out of unattended devices;
- use approved school communication channels;
- protect confidential and personal information;
- respect copyright and intellectual property;
- report loss, damage, suspicious messages or security concerns promptly; and
- obtain approval before installing software or applications.

Users must not:

- access, create, store or share illegal, harmful, hateful or inappropriate content;
- use another person's account;
- install unapproved software;
- interfere with the school network, filtering or monitoring systems;
- use technology to bully, harass, impersonate or exploit another person; or
- use personal email, messaging or social media accounts for communication with pupils.

8. Devices, Images and Communication

Personal mobile phones and smart devices must not be used by staff where pupils are present, in accordance with the Staff Code of Conduct and the Staff Acceptable Use Agreement in Appendix 1. Pupils must hand mobile phones to the School Office unless specific permission has been given. A pupil may bring and use a personal iPad or laptop for learning only where this has been approved by the Learning Development Department and Safeguarding Team, the device has been checked as required, and the pupil and parent or carer have signed the Personal Device Acceptable Use Agreement in Appendix 3. Permission may be withdrawn if the agreement is not followed.

Photographs, videos, or audio of pupils should be taken only on approved school devices wherever possible. They must have a legitimate school purpose, comply with consent and data-protection arrangements, and be stored and shared only through approved school systems. In exceptional circumstances, where a school device is unavailable and a staff member uses a personal device, the images must be uploaded to the designated school Teams folder within 24 hours and then permanently deleted from the personal device, including any cloud storage or 'recently deleted' folder. The images must not be retained, shared, or used for any other purpose. Further expectations relating to the taking, storing and sharing of images are included in the Staff Acceptable Use Agreement in Appendix 1 and the Pupil and Personal Device Acceptable Use Agreements in Appendices 2 and 3

School email, Microsoft Teams, Tapestry, iSAMS and other approved platforms must be used in accordance with school policies, access controls and professional expectations.

9. Social Media

Access to social media on school systems will be appropriately controlled. Official accounts may only be managed by authorised staff and must use approved school contact details.

Members of the school community must not use social media to disclose confidential information, bully or discriminate, impersonate another person, distribute misleading or manipulated content, bring the school into disrepute or communicate inappropriately with pupils.

Concerns will be managed under the relevant safeguarding, behaviour, anti-bullying, staff conduct or allegations procedures.

10. Responding to Concerns and Incidents

Any concern involving online behaviour, technology or AI must be reported promptly. Where a pupil may be at risk:

8. Report the concern immediately to the DSL or a deputy.
9. Make an accurate record.
10. Keep devices and potential evidence secure.
11. Do not view, copy, forward, print or delete suspected child abuse imagery.
12. Do not conduct an independent safeguarding investigation.
13. The DSL will assess the concern and follow the Safeguarding and Child Protection Policy.
14. Parents will be informed where appropriate and where this will not increase risk or compromise an investigation.
15. Children's Social Care, the Police, CEOP, the Internet Watch Foundation, the LADO or other agencies will be contacted where required.

If a child is in immediate danger or a crime is in progress, the Police will be contacted using 999. Concerns involving a member of staff must be reported to the Head without delay. Concerns involving the Head must be reported under the school's allegations and safeguarding procedures.

The school's response will be child-centred, proportionate and supportive. Online incidents will be addressed whether they occurred on or off site and whether they involved a school or personal device.

A breach of an Acceptable Use Agreement will be considered in accordance with the nature and seriousness of the incident and may result in restricted or withdrawn access to school systems or personal devices, alongside action under the relevant behaviour, safeguarding, staff conduct or disciplinary procedures.

11. Specific Online Safeguarding Concerns

The school will respond under its safeguarding procedures to concerns involving:

- cyberbullying and online harassment;
- sexual violence or sexual harassment online;
- the sharing or creation of nudes or semi-nudes, including AI-generated or digitally altered images;
- deepfakes, impersonation and manipulated media;
- online grooming, child sexual exploitation or criminal exploitation;
- harmful or illegal content;
- hate speech, discrimination, radicalisation or extremism;
- scams, coercion, blackmail or financial exploitation; and
- harmful interactions with AI chatbots or other automated systems.

Detailed operational procedures are contained in the Safeguarding and Child Protection Policy and local safeguarding procedures, rather than repeated in full within this policy.

12. Data Protection and Privacy

Personal data will be processed in accordance with applicable data-protection legislation and school policies. Staff and pupils must not enter the following into an AI tool unless the tool and specific purpose have been formally approved and a lawful basis and safeguards are in place:

- pupil names or identifying information;
- safeguarding records;
- health, SEND or pastoral information;
- photographs or recordings of pupils;
- assessment or behaviour records;
- staff or parent personal information; or
- confidential or commercially sensitive information.

Staff responsibilities for protecting personal data and reporting suspected data breaches are set out further in the Staff Acceptable Use Agreement in Appendix 1.

13. Monitoring and Review

This policy will be reviewed at least annually and sooner following a change in legislation or guidance, a significant incident, a change to systems or infrastructure, a new technological risk, or evidence that current arrangements require improvement.

Online safety and AI incidents, filtering and monitoring reports, training, pupil voice and safeguarding trends will inform the review.

Appendix 1: Staff Acceptable Use Agreement

Acceptable Use Policy (AUP) for Staff September 2026-27

Members of staff responsible: Head and DSL ICT Support Provider: Addooco (Managed ICT Services Provider) Review Date: October 2027

ICT (including data) and related technologies such as virtual classrooms, email, the internet and mobile devices are an expected part of our daily working life in S. Anselm's School. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT.

The School's ICT infrastructure, network security, systems monitoring, backup services and technical support are managed by Addooco, an accredited external ICT support provider. Addooco staff may, where necessary and authorised, access systems remotely for maintenance, troubleshooting, security monitoring and safeguarding purposes. All such access is subject to appropriate confidentiality, data protection and safeguarding requirements.

Staff Responsibilities

1. I will only use S. Anselm's School email, internet, learning platforms and any related technologies for professional purposes or for uses deemed reasonable by the Head or Governing Body.
2. I will comply with the ICT system security requirements (including Sophos protection and multi-factor authentication where implemented) and will not disclose any passwords provided to me by S. Anselm's School or other related authorities.
3. I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
4. I will use school channels at all times (such as school email) when communicating with pupils and parents on school matters.
5. I will only use the approved, secure email system(s) for any S. Anselm's School business or, in exceptional circumstances, with approval from two of the following: the Head, the Bursar and a Governor.
6. I will ensure that personal data (including information stored within iSAMS and other school systems) is kept secure and is used appropriately, whether in S. Anselm's School, taken off-site or accessed remotely. Personal or sensitive data taken off-site must be encrypted.
7. I will immediately report any actual or suspected data breach, cyber-security incident, loss of device, phishing attempt or unauthorised access to the Head, DSL, Bursar and/or Addooco as soon as it is identified.
8. I will ensure that devices used to access school systems are adequately protected with passwords, updated software and security measures approved by the School.
9. I will not install any hardware or software without permission of the School leadership team or Addooco.
10. I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
11. Images of pupils and/or staff will only be taken, stored and used for professional purposes in line with S. Anselm's School Safeguarding Policy and with appropriate consent from the parent, carer or staff member where required.
12. I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or the Head.
13. I understand that Addooco may monitor system performance, security alerts, network activity and system logs on behalf of the School to maintain the security, integrity and availability of school systems.
14. I understand that any files or messages stored on S. Anselm's School systems or devices may be removed if deemed inappropriate.
15. I will support S. Anselm's School approach to online safety and will not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the S. Anselm's School community.
16. I will respect copyright and intellectual property rights.
17. I will ensure that my online activity, both within and outside S. Anselm's School, does not bring my professional role or the School into disrepute.
18. I will support and promote S. Anselm's School Online Safety and Data Security Policy and help pupils to be safe and responsible in their use of ICT and related technologies.
19. I understand that it is my professional duty to read S. Anselm's School Online Safety and Data Security Policies and comply with the guidance contained within them.
20. I understand that cyber-security and data protection are shared responsibilities and that I may be required to complete training provided by the School or Addooco to maintain compliance and safeguard school systems and data.
21. I understand that this policy forms part of the terms and conditions set out in my contract of employment. I agree to follow this Code of Conduct and support the safe and secure use of ICT throughout the School.

Appendix 2: Pupil Acceptable Use Agreement

When using technology at S. Anselm's, I will:

- keep my password private;
- use technology only for the task I have been given;
- be kind and respectful online;
- keep personal information and images private;
- use only approved websites, applications and AI tools;
- use AI only when a teacher has permitted it;
- check AI answers because they may be inaccurate or unfair;
- say when AI has helped me with my work;
- never use AI to create fake, harmful or embarrassing content;
- never present AI-generated work as entirely my own;
- not bypass school security or filtering;
- take care of school equipment; and
- tell a trusted adult immediately if I see or receive something worrying.

Name: _____

Signature: _____

Date: _____

Appendix 3: Personal Device (iPad/Laptop) Acceptable Use Agreement

At S. Anselm's School, our priority is to keep all pupils safe, including when using digital devices. This agreement sets out clear expectations for pupils who bring and use a personal iPad or laptop in school. By signing this contract, you agree to follow the school's Code of Conduct for safe and responsible use.

Pupil Responsibilities

I understand that bringing a personal device into school is a privilege, and I agree to the following:

- I will keep my password secure and will not share it or allow others to use my account.
- I will only use my device for tasks set or approved by a teacher.
- I will not share personal information online.
- I will communicate politely and respectfully in all messages.
- I will ensure that my online behaviour does not offend or harm others.
- I will not access or use anyone else's account.
- I will not email, message, or communicate with people I do not know.
- I will immediately share any concerns about messages or content I encounter with a trusted adult.
- I will not take, use, or share images without a teacher's permission.
- I will respect the school's firewall, filtering systems, and security settings.
- I will only use applications and programmes that have been approved or directed by a teacher.
- I will take care of my device and use it responsibly at all times.
- I will only bring and use a personal device that has been approved and checked by the school's IT department.

Agreement

I understand that failure to follow this agreement may result in the withdrawal of permission to use my personal device in school and further action in line with the school's behaviour and safeguarding policies.

I agree to follow this Code of Conduct at all times when using my personal device at school.

Pupil Name: _____

Pupil Signature: _____ Date: _____

Parent/Carer Name: _____

Parent/Carer Signature: _____ Date: _____

Learning Development Department: _____ Date: _____

Safeguarding Team: _____ Date: _____