Exceed Learning Partnership
• EVERY CHILD • EVERY CHANCE • EVERY DAY •

ICT Acceptable Use Policy for Children/Young People

Status	**Statutory**
Version	**3**
Responsible Directors' Board	**Finance and Operations Committee**
Responsible Persons	**Deputy CEO and Director of ICT**
Date Policy Reviewed	**August 2025**
Next Review Date	**September 2026**
Academy to implement without Amendment, using appendix when required	

Summary of Changes from Previous Version

Version	Date	Author	Summary of Updates
V1			New Policy
V2	August 2024	Director of ICT	Updated to new template format. Updated all sections with new content to improve the content of the policy.
V3	August 2025	Director of ICT	Updated 'Safe and Secure Internet and Digital Platform Access' section to include reference to ethical use of AI Introduction of dedicated 'Artificial Intelligence (AI) Use' section New 'Parent' paragraph on page 8

Contents

Introduction

This policy outlines the acceptable use of Information and Communication Technology (ICT) resources within our school. The purpose is to ensure that all students and young people use ICT resources safely, responsibly, and in accordance with UK laws and the Department for Education (DfE) requirements, including those in *Keeping Children Safe in Education*. By adhering to this policy, students contribute to creating a safe and respectful learning environment, fostering responsible digital citizenship, and understanding the benefits and potential risks associated with online technologies.

Safe and Secure Internet and Digital Platform Access

The internet and digital platforms are powerful tools for learning, research, and communication. However, it is essential that students use these resources safely and responsibly. This section outlines how students can access these tools while maintaining the highest standards of security and ethical behaviour.

Expectations: Students are expected to use the internet and school-provided digital platforms strictly for educational purposes. They must not attempt to access inappropriate content or engage in activities that compromise the security of the school's network. Personal devices should only be used under the conditions set by the school. Students are also encouraged to promote digital wellbeing and healthy screen time habits.

- **Access and Monitoring**: Internet access within the school is monitored and filtered to protect students from inappropriate content. All usage is logged, and students should be aware that their online activities are subject to review by school staff. Students are encouraged to report any inappropriate content or suspicious activities encountered online to a staff member.
- **Responsible Use**: Students must use the internet and school-provided digital platforms for educational purposes only. Any form of misuse, including accessing inappropriate websites or engaging in illegal activities, is strictly prohibited. This also extends to the **appropriate and ethical use of Artificial Intelligence (AI) tools** for educational purposes, ensuring proper citation and avoiding plagiarism. Students should critically evaluate information from all digital sources, including AI-generated content.
- **Cloud-Based Services**: When using school-approved cloud-based services and applications, students must adhere to guidelines regarding data storage, sharing, and privacy. All content uploaded or shared on these platforms should be appropriate and directly related to educational tasks.
- **Personal Devices**: Personal devices may only be connected to the school network with prior permission from ICT staff. All devices must comply with the school's security protocols, including having up-to-date operating systems and security patches.

Electronic Communication (Email, Chat, SMS)

Electronic communication in any format is an important tool for communication within the school community. Proper use of electronic communication tools ensures effective communication, while poor usage can lead to misunderstandings, security breaches, and even cyber bullying. This section highlights how students should use electronic communication respectfully and responsibly.

Expectations: Students must use their school email accounts (Where provisioned) for academic-related communication only.
Emails, Chat, SMS messages and any online posting should be written with professionalism, respecting both the recipients and the purpose of the communication. Students must be vigilant about online security and avoid opening suspicious emails or attachments from unknown senders.

- **School Email Accounts**: Students are provided with school email accounts to be used solely for educational communication. Personal use of school email accounts is not permitted.
- **Professional Communication**: All electronic communication should be written with respect and professionalism. Abusive, offensive, or harassing language is not tolerated.
- **Security**: Students must not open emails or attachments from unknown sources as they may contain harmful software. Phishing and other forms of online scams should be reported immediately.
- **Phishing** and other forms of online scams should be reported immediately to a staff member. Students should be aware of common signs of phishing, such as suspicious links, unusual sender addresses, or requests for personal information.

Cyber Security

Cyber security is crucial in protecting personal information and ensuring the integrity of the school's network. Understanding and adhering to good security practices is essential for all students. This section explains how students can contribute to a secure digital environment.

Expectations: Students are expected to create and maintain secure passwords, use only school-approved software, and refrain from tampering with the school's network or security systems. They must respect the privacy and security of others by not accessing, modifying, or deleting other users' files.

- **Passwords**: Students are required to create and maintain strong passwords and keep them confidential. Sharing passwords or using someone else's account is strictly prohibited. Where implemented, students must also protect their two-factor authentication (2FA) methods.
- **Software and Updates**: Only school-approved software should be installed on devices. Students must not attempt to bypass security measures or interfere with the school's network.
- **Data Protection**: Students must not access, modify, or delete other users' files. Sensitive information, such as personal data, should not be shared without appropriate authorisation, in line with General Data Protection Regulation (GDPR) principles.

Photographs & Video Recording

Taking and using photographs and videos can be a valuable educational tool but must be done in a way that respects the privacy and dignity of everyone involved. This section explains the rules surrounding the use of school equipment for recording and the strict prohibition on using personal devices for such purposes.

Expectations: Students should only take photographs or videos with school equipment and after obtaining

proper consent. The use of personal devices to record within the school is prohibited unless specifically authorized. Students must not share or distribute images or videos without permission, as this could lead to serious privacy violations and disciplinary action.

- **School Equipment**: Students may use school-provided equipment to take photographs and video recordings for educational purposes with prior consent from teachers and all individuals involved.
- **Prohibited Use of Personal Devices**: The use of personal mobile phones or any other devices to record photographs or videos of students, staff, or school premises is strictly prohibited unless explicitly authorised by school.
- **Sharing and Distribution**: Unauthorised sharing or distribution of images or videos, especially those depicting students or staff, is not allowed and may result in disciplinary action. Students must be aware of the ethical implications of digitally altering images or videos, and the creation or distribution of misleading content such as "deepfakes" is strictly prohibited. Any authorised recording must be used solely for the agreed educational purpose and not for personal social media or other platforms.

Cyber Bullying

Cyber bullying is a serious offense that can cause significant harm to individuals. The school is committed to preventing and addressing all forms of bullying, including those that occur online. This section defines cyber bullying, emphasizes the importance of reporting it, and outlines the school's response to such incidents.

Expectations: Students must not engage in any form of cyber bullying. They are encouraged to report any incidents of cyber bullying immediately, whether they are victims or witnesses. The school will act promptly to support victims and address the behaviour of those involved in bullying, in line with the school's anti-bullying policies. Students are encouraged to be **'upstanders'** by supporting victims and challenging bullying behaviour safely and appropriately.

- **Definition**: Cyber bullying is the use of digital technology, including social media, messaging, and email, to harass, threaten, or humiliate others. This behavior is unacceptable and will not be tolerated.
- **Reporting**: Students who experience or witness cyber bullying should report it immediately to a trusted staff member, safeguarding lead, or through the school's designated reporting channels.
- **Support and Consequences**: The school will provide support to victims of cyber bullying and take appropriate disciplinary action against perpetrators, in line with the school's anti-bullying policy. The school acknowledges the potential mental health impact of cyber bullying and will offer appropriate support to affected students.

Artificial Intelligence (AI) Use

Artificial Intelligence tools are rapidly evolving and can be powerful aids for learning. This section outlines the school's expectations for the responsible and ethical use of AI by students, ensuring academic integrity and critical thinking.

Expectations

Students are encouraged to explore and utilise AI tools to support their learning, but always with transparency, critical evaluation, and adherence to academic integrity. AI should be used to augment, not replace, original thought and effort.

Ethical AI Use

- Transparency and Attribution: When AI tools are used to generate content (e.g., text, code, images, ideas) that contributes to assessed work, students *must* explicitly acknowledge the use of AI. This includes citing the specific tool used and describing how it was employed, similar to citing other sources. Specific guidelines for referencing AI-generated content will be provided by subject teachers.
- Original Thought vs. Augmentation: AI tools should be used to *aid* learning and research (e.g., for brainstorming, summarising complex texts, explaining concepts, checking grammar). They must not be used to complete entire assignments or tasks where the primary objective is to demonstrate a student's own understanding, analytical skills, or original creative work without significant personal contribution.
- Critical Evaluation: AI outputs can contain errors, biases, or misinformation. Students are responsible for critically evaluating any information or content generated by AI, cross-referencing it with reliable sources, and understanding that AI responses are not always factually accurate or unbiased.
- Bias Awareness: Students should be aware that AI models can reflect biases present in their training data. Therefore, AI-generated content should not be accepted uncritically.

Academic Integrity and AI Misuse

- Definition of Misuse: Submitting work entirely or substantially generated by AI without proper attribution, or using AI to circumvent the learning objectives of an assignment (e.g., generating an essay to avoid the writing process) will be considered academic misconduct.
- Consequences: Any misuse of AI that violates academic integrity will be dealt with according to the school's existing academic misconduct and disciplinary policies, which may include redoing assignments, grade penalties, or other disciplinary actions.
- Detection: Students should be aware that the school may employ various methods to identify the misuse of AI in submitted work.

Data Privacy and Confidentiality with AI

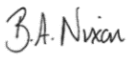
Students must never input personal, sensitive, or confidential information (e.g., full names, home addresses, private conversations, school-specific data, or information relating to other individuals) into public AI tools or platforms, as this data may be used for model training and could compromise privacy.

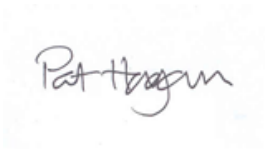
Summary

By following the guidelines set out in this ICT Acceptable Usage Policy, students will contribute to a safe and effective learning environment. Adherence to this policy is mandatory, and violations may lead to disciplinary action. Students and parents must review this policy and sign an acknowledgment form, demonstrating their understanding and commitment to these rules.

Parents are encouraged to support their children in adhering to this policy, both at school and at home. As the ICT landscape is constantly evolving, this policy is a living document that will be reviewed and updated regularly.

Policy Reviewed: August 2025

Signed Chief Executive: 

Signed: Chair of Directors: 

Policy to be reviewed in September 2026