Status:	Regulatory
Applies to:	Senior School
SLT Reviewer (initials):	CW
Committee Monitor:	Education

ICT Acceptable Use Policy (Pupils and Parents)

Independent Day and Boarding School for Girls & Boys aged 3 to 18 years

September 2008

Reviewed April 2025

ICT Acceptable Use Policy (Pupils and Parents)

1 Introduction

All pupils and their parents will be asked to sign the ICT Acceptable Use Policy Agreement.

1.1 This policy aims to ensure that:

1.1.1 Pupils use ICT resources responsibly and safely.

1.1.2 School ICT facilities and users are protected from accidental or deliberate misuse.

1.1.3 Clear guidelines are set for the use of mobile phones, smart devices and portable electronic devices for pupils, staff, parents/carers and volunteers via the signed declaration attached to this policy, school assemblies and parental communication.

1.2 Key concerns

1.2.1 This policy aims to address some of the challenges posed by mobile phones, smart devices and electronic devices whilst in school, such as:

1.2.2 Risks to child protection.

1.2.3 Data protection issues.

1.2.4 Risk of theft, loss, or damage.

1.2.5 Ensuring that the use of technology is appropriate, purposeful, and supports teaching and learning.

2 Legal Framework

2.1 Statutory Legislation

This policy complies with, but is not limited to, the following statutory legislation:

2.1.1 General Data Protection Regulation (GDPR).

2.1.1.1 Any images or videos recorded at the school must not be shared or uploaded to the internet or social media without the school's written permission.

2.1.1.2 Images of pupils or staff stored on the school's ICT equipment are considered personal data and are protected by the school's GDPR policy. This data must not be shared or distributed without prior written consent from the school.

2.1.2 Data Protection Act 2018.

2.1.3 Defamation Act 2013.

2.1.4 Protection of Freedoms Act 2012.

2.1.5 Keeping Children Safe in Education (September 2024).

2.2 The school reserves the right to amend this ICT Acceptable Use Policy at any time and in keeping with the overall school policy.

2.3 The school reserves the right to change, update or withdraw the school's ICT resources and facilities.

2.4 For the purposes of this document, Stover Community refers to all pupils, and staff members employed by Stover School.

3 General ICT Use Rules

3.1 The school defines acceptable use as activities that directly or indirectly support the educational needs of the learner.

3.2 The school reserves the right at any time to monitor all users' network access and inspect all data including that stored on personal directories.

3.3 Access to school ICT facilities is a privilege and must comply with this policy.

3.4 Internet use during school hours is for educational purposes only and as directed by staff members.

3.5 Uploading or downloading executable files, music, or media without permission from a member of the IT department is prohibited.

3.6 It is prohibited to upload or download music, video files or any other media without first ensuring it is not protected by copyright (a lack of copyright statement is not evidence of a lack of copyright) to the school network.

3.7 Accessing inappropriate or illicit websites, including but not limited to those containing pornography, violence, extremist content, illegal downloads, or gambling, is strictly prohibited.

3.8 Any misuse of ICT facilities or services must be immediately reported to a staff member.

3.9 Pupils are responsible for logging off from school devices after use and leaving computers tidy.

3.10 It is prohibited for pupils to work on a device that still has an open active session from a previous user.

3.11 Sharing passwords, using another person's account or theft of digital identity is prohibited.

3.12 Pupils must not change or delete information on shared drives unless told to do so by a member of staff.

3.13 Personal data storage devices must be clean, virus-free, and devoid of inappropriate content.

3.14 Any violation of these rules may result in disciplinary action.

4 Email Use

4.1 School email accounts may be monitored by the IT Manager and as instructed by a member of the Senior Leadership Team.

4.2 Pupils and staff must use their school email accounts for all school-related correspondence.

4.3 Pupils may only send emails or messages to people they know, or else with staff permission. Messages must be polite, responsible, and free of personal information.

4.4 Pupils should immediately report inappropriate emails to a member of staff.

4.5 Pupils must not allow others to access their email accounts.

5 Online Safety

The school recognises the importance of safeguarding pupils from online risks and adopts a whole-school approach to online safety. This is integrated into safeguarding policies, curriculum planning, staff training, and parental engagement.

The school's ICT Acceptable Use policy works alongside its child protection measures to ensure pupils remain safe, whether online or offline, and promotes responsible use of technology at all times.

5.1 Key Online Safety Risks:

5.1.1 **Content**: Exposure to harmful material such as extremism, self-harm, or inappropriate images.

5.1.2 **Contact**: Harmful interactions for purposes of grooming or sexual exploitation.

5.1.3 **Conduct**: Behaviour that heightens the risk of harm or directly causes it. This includes actions such as the creation, distribution, and receipt of explicit images (both consensual and non-consensual, including nudes, semi-nudes, and pornography), as well as the sharing of other explicit content and/or engaging in online bullying.

5.1.4 **Commerce**: Risks such as phishing, scams, inappropriate advertising or online gambling.

5.2 School System Provisions

5.2.1 IT systems include appropriate filtering and monitoring of internet access to mitigate risks while supporting learning activities.

5.2.2 Pupils are educated on responsible internet use, including understanding the dangers of harmful online content and the implications of unsafe behaviour.

5.2.3 Clear rules govern the use of mobile and smart technology on school site.

5.2.4 Cyberbullying, sharing explicit material, and accessing inappropriate content are strictly prohibited and will result in disciplinary action.

6 Cyberbullying

Bullying, intimidation, and harassment via mobile phones, smart devices or other online devices are complex challenges for schools. The school addresses such incidents in line with its Anti-Bullying Policy. These rules apply to device use both inside and outside school.

6.1 Examples of cyberbullying offences include:

6.1.1 Filming or photographing others to humiliate, embarrass, or intimidate them.

6.1.2 Sharing content online that humiliates, embarrasses, intimidates others.

6.1.3 Sharing images online that compromise pupil safety including sharing personal details, such as home address, friendship groups, or lifestyle patterns.

6.1.4 Bullying or harassment by messages or posts via text, email, or social media - including where no thought to the risks to others has been considered.

6.1.5 Making disrespectful comments, misrepresenting events, or posting defamatory remarks about any members of the Stover community.

6.1.6 The creation of inappropriate images and media including those generated by AI (deepfake).

6.1.7 Publishing photos of vulnerable pupils, such as those with SEND status or on child protection plans, potentially putting them at risk.

6.1.8 Wasting time or causing disruption by engaging in cyberbullying offences.

6.2 **Cyberbullying and the Law**

By committing an act of cyberbullying, a person may be committing a criminal offence under a number of different acts. These include (but are not limited to) the following:

6.2.1 Malicious Communications Act 1988

6.2.2 Communications Act 2003

6.2.3 Public Order Act 1986.

6.2.4 Criminal Justice and Public Order Act 1994

6.2.5 Protection from Harassment Act 1997

6.2.6 Defamation Act 2013

7 Social Media Code of Conduct

7.1 Breaches of this code will be taken seriously. Illegal, defamatory, or discriminatory content may lead to police involvement and possible prosecution.

7.2 Pupils, parents and carers must behave responsibly online and avoid defamatory posts on all social media sites or online.

7.3 Complaints about the school including its values and methods should follow the official Complaints Policy, not be shared on social media or messaging apps (e.g., WhatsApp, Signal, Telegram).

7.4 The sharing of abusive messages concerning individuals via messaging apps, will not be accepted.

7.5 With parental permission, the Head may review messages exchanged among parents to address problems promptly and effectively.

7.6 If issues persist, the Head may request the closure of group chats involving parents or parental bodies.

7.7 Pupils and parents/carers must not attempt to 'friend' or 'follow' staff on social media.

7.8 Posting anonymously or under an alias to avoid accountability is not allowed.

7.9 The school may request the removal of harmful material from social media platforms.

8 Use of Generative Artificial Intelligence (AI) Tools

At Stover School, we recognise the potential of generative Artificial Intelligence (AI) tools, which include standalone products (e.g., ChatGPT, Copilot) and AI integrated into productivity suites. Generative AI is defined as a specific type of AI capable of creating new data or content similar to human-produced outputs. While these tools can enhance education and foster innovation, their use must be guided by clear ethical principles and an understanding of their limitations.

8.1 **Opportunities and Risks**.

8.1.1 Generative AI may be used to enhance learning and support pupils. However, we are mindful that AI can be inaccurate, biased, and potentially amplify existing discriminatory viewpoints.

8.1.2 Staff and pupils will exercise vigilance in identifying and addressing such biases in AI-generated content.

8.1.3 While AI can assist in many areas, it is not a replacement for human creativity, intuition, or understanding.

8.2 **Academic Integrity**:

8.2.1 AI tools must not be used for cheating, submitting work that is not your own without proper attribution, or engaging in any other unethical behaviour.

8.2.2 Any content produced with AI must reflect the individual's understanding and effort.

8.2.3 Failure to attribute AI-generated content in coursework or other assessments completed as part of an external examination (such as

GCSE, A Level, BTEC or equivalent) will be regarded as malpractice and reported to the relevant examination board, which may result in disqualification. Pupils and staff are required to follow the JCQ Guidance on the Use of AI in Assessments.

8.3 Ethical Use

AI tools must not be used to impersonate individuals or organisations, generate harmful, offensive, or unlawful content, or mislead others.

8.4 Compliance with School Policies:

The use of AI tools must align with our Anti-Bullying, Exams and Behaviour Policies, and all other relevant school policies, as well as statutory legislation.

8.5 AI Misconduct

8.5.1 Pupils are strictly prohibited from using Artificial Intelligence (AI) tools to create or distribute content that is discriminatory, harmful, offensive, or intentionally biased.

8.5.2 AI-generated content must not substitute pupil effort or original work, and copying or paraphrasing AI outputs to the extent that the work is no longer the pupil's own is prohibited, and will be considered malpractice.

8.5.3 Pupils who fail to use AI tools responsibly may face sanctions. These could include consequences at an internal school level or external actions if the work is submitted for broader assessment purposes.

8.5.4 Any suspected misuse of AI in non-examined formal assessments will be reported to the relevant awarding body, in line with JCQ Guidance and Stover schools Exam Policy.

9 BYOD (Bring Your Own Device)

9.1 General BYOD Rules

9.1.1 BYOD include but are not limited to laptops, chromebooks and tablets.

9.1.2 The school reserves the right at any time to monitor, audit, inspect and if necessary, confiscate any BYOD brought onto school grounds.

9.1.3 Parents or bill payers are responsible for monitoring their child's BYOD and ensuring they follow age restrictions on apps especially regarding the internet and social media. We encourage parents/carers to discuss appropriate use and security with their child.

9.1.4 Software and apps on any BYOD must comply with copyright and licensing laws.

9.1.5 Personal devices are not covered by the school's insurance and are brought to school at the owner's risk. The school will not be held responsible under any circumstance for personal devices and are the sole responsibility of the pupil and their parents/guardians.

9.1.6 Costs of replacement or repair due to loss or breakage, accidental or otherwise, of personal devices (not part of a Stover school leasing scheme) will be met by the pupil/parents/guardians and not the school.

9.2 Laptops and Chromebooks

9.2.1 All pupils in Year 10 and above are expected to bring a laptop or chromebook to school to support their learning in class.

9.2.2 In addition, pupils across the school may be given permission to use a laptop or Chromebook as a learning support tool. Permission must be pre-arranged and agreed upon by a member of the Learning Support Team as part of an LS Pupil Profile.

9.2.3 BYO devices must only be used to support learning in class. Pupils are not permitted to use a BYOD in the toilets, changing rooms, during break periods or whilst travelling on a school minibus or coach within the hours of 8.30am and 4.30pm.

9.2.4 A BYOD is a privilege that can be withdrawn. Any pupil who misuses this privilege will not be permitted to bring their device into school, temporally or in some cases permanently.

9.2.5 The school reserves the right at any time to monitor, inspect and if necessary, confiscate any device brought onto school grounds.

9.2.6 The school reserves the right to install monitoring and filtering software onto a BYOD for the sole purpose of preventing access to inappropriate material during school hours.

9.2.7 All BYOD must only access the internet via the schools' network whilst on school site, for monitoring and filtering purposes.

9.3 Mobile Phone Policy

9.3.1 In line with government guidelines, mobile phones and smartwatches, (or similar internet-enabled devices) are prohibited from being used in school between the hours of 8:30 and 4:30, whilst on school premises or during a school-led activity, including fixtures and school trips.

9.3.2 These devices must be switched off and stored in the pupil's locker or school bag, and must not be carried on their person during these hours.

9.3.3 Permission for use may be granted by a member of staff for a specific named purpose or task and whilst under the supervision of a member of staff.

9.3.4 The school reserves the right to amend this mobile phone policy in accordance with current government guidelines.

9.4 BYOD and Mobile Phone Compliance and Consequences

9.4.1 Any confiscated item will be stored securely in the main school office.

9.4.2 The period during which breaches are counted, spans one academic year.

9.4.3 On the first infringement of this policy, the mobile phone, smart device or BYOD will be confiscated. The pupil can collect it at 4.30pm on the same day.

9.4.4 On the second infringement, the device will be confiscated, and an email will be sent to parents/carers informing them of the incident and warning of the consequences of further breaches.

9.4.5 On the third infringement, the device will be confiscated, parents will be contacted and the pupil will receive a Head of Key Stage sanction.

9.4.6 Repeated infringements - the device will be confiscated, parents will be informed, and the pupil will receive a sanction determined by the Head of School. This may include the withdrawal of permission to bring the device into school, or a requirement to hand in the device during school hours, for a specified period.

9.4.7 Serious breaches, especially involving bullying, will be dealt with under the school's behaviour policy. Parents/carers will always be informed, and the severity of sanctions will depend on the situation. The school may contact outside agencies such as the police, social services, or Childnet if needed.

9.4.7.1 Evidence of the offence will be preserved if necessary, and victims are encouraged to keep screenshots.

9.4.8 Refusal to comply with these rules will be treated as deliberate defiance of school expectations and may result in more serious sanctions, in accordance with the school's behaviour policy.

10 Declaration and Agreement Form

Pupil Details	
Pupil name:	
Year group/class:	
Parent(s) name(s):	

I _____ (name of parent/carer),

parent/carer of _____(name of child), declare that I have received, read and understood the terms and conditions of the ICT Acceptable Use Policy.

I understand my obligations of this policy and agree to comply fully with them whilst my child is a pupil at Stover School.

I understand that if my child fails to abide by the terms and conditions of the ICT Acceptable Use Policy that their personal device may be confiscated and that the school reserves the right to revoke the permission of my child to bring their personal device into school.

Pupil Signature: _____

Parent/Carer Signature: _____

Date:_____