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

STOVER SCHOOL

ICT Acceptable Use Policy (Pupils)

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

September 2008
Reviewed November 2024

Stover Pupil ICT Acceptable Use Policy

The ICT Acceptable Use Policy intends to ensure that:

1.0 Introduction to the policy

1.1 Pupils will be responsible users and remain safe when using ICT equipment, resources and services.

1.2 The school ICT facilities and users are protected from accidental or deliberate misuse which could jeopardise their safety, security and integrity.

1.3 The policy aims to promote, and set an example for, safe and responsible phone/smart device use.

1.4 Set clear guidelines for the use of mobile phones, smart devices and portable electronic devices for pupils, staff/carers, parents and volunteers.

1.5 Support the school's other policies, especially those related to child protection and behaviour.

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

- Risks to child protection
- Data protection issues
- Risk of theft, loss, or damage
- Appropriate use of technology

2.0 Legal framework.

1. This policy has due regard to statutory legislation, including, but not limited to, the following:
2. General Data Protection Regulation (GDPR)
3. Data Protection Act 2018
4. Defamation Act 2013
5. Protection of Freedoms Act 2012
6. Keeping Children Safe in Education (September 2022)

2.7 All pupils and parents will be asked sign the ICT Acceptable User Policy Pupil/ Parent Agreement

3.0 ICT Acceptable Use Policy

3.1 Stover School's ICT Acceptable Use policy provides the rules of behaviour for the use of the school's ICT resources and facilities.

3.2 Access to Stover School's ICT resources is granted at the discretion of the school and is provided on condition that each user acts accordingly and in line with the policies concerning these facilities.

3.3 Access to the school's ICT facilities is a privilege and not a necessity

3.4 Access to the internet during the school day is for educational purposes only, and is permitted as instructed by the teacher

3.5 It is prohibited to upload or download executable files to the school network without the explicit permission of the Systems Manager or the Head of Computer Science, as these may contain malicious content such as virus.

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 It is prohibited to access websites containing video, images and content which is not age appropriate or any illicit or unsuitable material

3.8 Any misuse of ICT facilities or services should be reported to the school

3.9 Access to the school network entails personal responsibility and compliance with all school rules and the school's acceptable use policy

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

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

3.12 The school reserves the right to amend the ICT Acceptable Use policy at any time and in keeping with the overall school policy

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

3.14 Pupils must use their designated network account when using the school's ICT facilities and services, and must not use the account of any other person

3.15 It is prohibited for pupils to divulge their network account details to anyone except a teacher or the school's ICT support staff. Pupils must never divulge their passwords

3.16 It is prohibited for pupils to amend or delete any information that is stored on any shared drive other than their personal home share, unless specifically instructed to do so

3.17 All pupils will ensure they log off from every computer they use once they have finished their work

3.18 All pupils will ensure that they leave computers in a tidy and useable state

3.19 It is prohibited for pupils to work at a computer that still has an open active session from the previous user. They must log it off or bring it to the attention of the teacher

3.20 Pupils are prohibited from using the network in any way which would cause detrimental effect to the network or other users

3.21 It is the parent's/guardian's and pupil's responsibility to ensure that any portable data storage drive conforms to the requirement of the school. It should be fit for purpose, safe, clean and virus free. The drive must be free of illicit or unsuitable material

3.22 Any violation of the school's rules or policies regarding the school's ICT facilities is unacceptable and will result in disciplinary action as determined by the school and in line with the school's Behaviour Policy

4.0 School Emails

4.1 Staff and pupils have an individual email account. All Network Users must use their school email account for all school related correspondence.

4.2 Where necessary, email accounts may be monitored by the Network Manager. Pupils should immediately report any inappropriate emails they receive to their tutor or one of the pastoral team.

4.3 Pupils must only send e-mails/messages to people known to themselves or with the permission of a member of staff. E-mails/messages should polite and responsible and must not contain any personal information about themselves.

4.4 **E**mails should be polite and written with consideration for the person receiving my message. Pupils should not allow anyone else to use their email account.

5.0 Data Protection

5.1 Any images or video data which has been recorded at the school must not be transmitted or uploaded to the internet at any time without the school's written permission.

5.2 Any Images of pupils or staff which are held on the School's ICT equipment are to deemed personal data and covered by the school's GDPR policy. Under no circumstances is this data, as defined above, to be distributed without prior written consent from the school.

6.0 BYOD (Bring Your Own Device) Policy

6.1 At Stover School we encourage pupils in Year 10 and above, to bring their own laptop or tablet into school.

6.2 It is important to note that this is a privileged that could be withdrawn. Any pupil who minuses their device will not be permitted to bring it into school temporally or in some cases permanently.

6.3 We recognise that mobile phones are an important part of everyday life for our young people. We acknowledge that parents/carers may give their child(ren) mobile phones to protect them from everyday risks involving personal security and safety. Many pupils commute long distances to school and/or take part in extra-curricular activities outside normal school hours. We are also very aware that that mobile phones in school can be a distraction for pupils.

6.4 *Allowing access to mobiles in school introduces complexity and risks, including distraction, disruption, bullying and abuse, and can be a detriment to learning. Headteachers should consider restricting or prohibiting mobile phones to reduce these risks*. Behaviour in Schools advice from Department for Education July 2022

7.0 Responsibility with BYOD

7.1 It is the responsibility of pupils who bring mobile phones or smart devices to school to abide by the guidelines outlined in this document.

7.1.1 Pupils are instructed that if they do bring mobile phones (or other such electronic devices including smart watches) to school, <u>they are switched off and stored in either a bag or locker</u> from 8.30am until 4.30pm whilst on the school site.

7.2 Pupils are not permitted to use a mobile phone or smart device in the toilets, changing rooms or whilst travelling on a school minibus or coach within the hours of 8.30am and 4.30pm.

7.3 It is the responsibility of the parents or bill payer to monitor frequently, the activity on the mobile phone or smart device and to be aware of the age restrictions on applications in reference to the internet and Social Media. We encourage parents/carers to talk to their child about appropriate use and security.

7.4 Personal devices are not covered by the school's insurance and are brought in to school at the owner's risk.

7.5 The school will not be held responsible under any circumstance for a personal mobile device or for its use. Any personal mobile devices brought to the school under Bring Your Own Device (BYOD) initiative are the sole responsibility of the

pupil and their parents/guardians. Costs of replacement or repair due to loss or breakages accidental or not will be met by the pupil/parents/guardians.

7.6 Compliance with BYOD

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

7.8 *On the first infringement* of this policy, a record will be made of the incident, the mobile phone/smart device would be confiscated by a member of staff and stored in main reception. The device can be collected by the pupil at 4.30pm on the same day.

7.9 *On the second infringement*, the mobile phone/smart device would be confiscated by a member of staff and stored in main reception. A record will be made of the incident and an email will be sent to parents/carers to inform them and warn of the implications of a further breach of rules on mobile phones/smart devices.

7.10 *On the third infringement*, the mobile phone/smart device would be confiscated by a member of staff and stored in main reception. Parents/carers will be informed of the situation and the how and when the smart phone/smart device is returned to the pupil will be discussed with the parents.

7.11 Repeated infringements will be discussed with the parent/carer and a decision will be made by the school whether or not to withdraw the agreement to allow the pupil to bring the phone/device into school.

7.12 Serious breaches in conduct, particularly involving bullying, will be dealt with in accordance with the school's behaviour policy. In such cases, parents/carers will always be notified. The sanctions for more serious incidents will vary and will depend on the circumstances, the offence, and the degree to which trust has been breached. At this point the school may decide to contact outside agencies such as the Police, Social Services, Childnet, etc

7.13 If required, evidence of the offence will be preserved. Victims will be encouraged to keep screenshots for this purpose.

7.14 Refusal to comply with the rules included in this policy will be treated as refusal to follow instruction and may result in a more serious consequences in line with the school's Behaviour Policy.

8 Online Safety

8.1 It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

8.2 The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk (the four C's):

8.3 **Content**: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

8.4 **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

8.5 **Conduct**: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

8.6 **Commerce:** risks such as online gambling, inappropriate advertising, phishing and financial scams. If you feel you are at risk at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

8.7 Online concerns can be especially complicated and support is available from: **Internet Watch Foundation**: If the incident/report involves sexual images or videos that have been made and circulated online, the victim can be supported to get the images removed by the Internet Watch Foundation (IWF) https://www.iwf.org.uk/

8.8 **Childline/IWF Report Remove** is a free tool that allows children to report nude or sexual images and/or videos of themselves that they think might have been shared online https://www.iwf.org.uk/our-technology/report-remove/

9.0 Cyberbullying

9.1 Bullying, intimidation and harassment using a mobile phone or smart device represents a challenge for schools to manage, both in scale and complexity. The school will approach such incidents following the principles and procedures laid out in the school Anti Bullying Policy.

9.2 Rules on bullying, harassment, and intimidation apply to how you use your mobile phone or smart device even when you are not in school.

9.3 Examples of misuse include but are not limited to:

9.4 The deliberate engineering of situations where people's reactions are filmed or photographed in order to humiliate, embarrass or intimidate by publishing to a wider audience on social networking/messaging sites,

9.5 Bullying or harassment by text, image, video and email messaging; The posting of material on social networking/messaging sites, examples listed on Appendix 1 with no thought to the risks to personal reputation and sometimes with the deliberate intention of causing harm to others;

9.6 Making disrespectful comments, misrepresenting events or making defamatory remarks about teachers, other adults at school or fellow pupils;

9.7 General disruption and wasted time of those involved in solving the problems caused by the above;

9.8 Publishing photographs of vulnerable pupils who may be on a child protection plan or have a SEND status, where this may put them at additional risk.

9.9 It is important to note that the safety of pupils could be compromised through online sharing of images if a third party is able to determine their identity and/ or personal details such as home address, friendship group of lifestyle patterns.

10 Cyberbullying and the Law

By committing an act of cyber bullying, a person may be committing a criminal offence under a number of different acts. This includes the following:

10.1 **Malicious Communications Act 1988** Section 1 of the Malicious Communications Act 1988 states that it is an offence for any person to send a communication that is "indecent or grossly offensive" for the purpose of causing "distress or anxiety to the recipient". The Act also extends to threats and information which is false and known or believed to be false by the sender of the communication. A person found guilty of this offence is liable to receive a prison sentence of up to 6 months, a fine (currently of up to £5,000) or even both.

10.2 **Communications Act 2003** Section 127 of the Communications Act 2003 makes it a criminal offence to send via any electronic communication network a message or other matter that is deemed "grossly offences or of an indecent, obscene or menacing character". If found guilty of an offence under section 127 of the Communications Act 2003, a person can receive up to six months in prison, a fine or both.

10.3 **Public Order Act 1986.** Under section 5 of the Public Order Act 1986, it is an offence to use threatening, abusive or insulting words, behaviour, writing or any visual representations likely to cause harassment, alarm or distress within the hearing or sight of a person. With regards to cyberbullying, this offence could apply where the camera or video functionality now found on the vast majority of mobile phones is used as a way of causing such harassment, alarm or distress.

11 Social Media Code of Conduct

11.1 We understand the benefits of using social media; however, if misused, members of the school community can be negatively affected, as can the school's reputation.

11.2 This code of conduct sets out clear procedures for how we expect pupils and parents to conduct themselves on social media, such as Facebook, Twitter and when using messenger apps, such as WhatsApp, Snapchat, text messages and other social media apps.

11.3 Stover School expects pupils/parents/carers to behave in a civilized nature online and will not tolerate any of the following behaviour online: -

11.4 Posting defamatory 'statuses' about fellow parents/carers, pupils, the school or its Employees.

11.5 Complaining about the school's values and methods on social media. The school has Complaints Policy in place, to avoid parents/carers broadcasting grievances online and the policy is expected to be used.

11.6 Pupils/ parents/carers will be made aware of their responsibilities regarding their use of social networking and their conduct online.

11.7 Breaches of this code of conduct will be taken seriously by the school and, in the event of illegal, defamatory, or discriminatory content, breaches could lead to the police being informed and a prosecution.

11.8 Pupils/ parents/carers will not attempt to 'friend' or 'follow' any member of staff on social media.

11.9 Pupils/ parents/carers are asked not to post anonymously or under an alias to evade the guidance given in this code of conduct.

11.10 Stover School retains the right to request any damaging material to be removed from social media websites.

12 Online messaging

12.1 Stover School expects pupils, parents/carers to use messaging apps, such as WhatsApp, for purposes beneficial to themselves and the school, and will not accept any of the following behaviour:

12.2 Sending abusive messages to fellow pupils/parents/carers
12.3 Sending abusive messages about members of staff, parents/carers or the school.
12.4 Sending abusive messages to members of staff.

12.5 Should any problems arise from contact over messaging apps, the school will act quickly by contacting parents directly, to stop any issues continuing. Stover School can request a meeting with parents/carers if any misconduct, such as sending abusive messages or posting defamatory statuses, occurs online.

12.6 The school's complaints procedure will be followed as normal if any members of the Governing Board cause any discrepancies through their conduct whilst using online
messaging. The Headteacher can, with the permission of the parent/carer, view messages sent between members of the parental body in order to deal with problems quickly and effectively.

12.7 The Headteacher can request that 'group chats' are closed down should any problems continue between parents/carers or parental bodies.

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 user agreement 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 the terms and conditions of the ICT user agreement policy that their mobile phone and/ or tablet 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:_____