Sidcot Acceptable Use Policy (Students)

Sidcot School Digital Technology Acceptable Use Policy (AUP)

Sidcot School believes that effective use of Digital Technology is essential in enhancing learning across the curriculum. Excellent use of Digital Technology allows students to:

- Learn in an effective way
- Utilise the power of multimedia and interactivity to be motivated and learn
- Gain access to a wide range of resources and research
- Communicate easily with teachers, students and people outside the school environment
- Present work in a professional manner
- Develop innovation and problem solving skills
- Meet some additional educational needs.

However, there are potential accompanying dangers for students and staff. This policy has been written to ensure that Digital Technology is used effectively whilst minimising risk. Students and staff are advised and expected to take personal responsibility for their own use of Digital Technology. Before using any school Digital Technology equipment (or privately owned equipment) all students must complete this form and return it to the school. By signing this agreement, students agree to abide by its rules. The school will take appropriate action; should any of these rules be broken or there be any other cause for concern;. Where necessary the police and/or other authorities will be informed.

Use of Equipment

- Students are expected to treat Digital equipment carefully and not act in any way that might cause damage.
- Students are to use school equipment for work purposes only during the school day.
- Students are to report any faults or damage found with school equipment to itsupport@commercial.co.uk using their @sidcot.org.uk school email address.
- Students must not disclose their school system password to anyone else.
- Students must not use or attempt to use another person's sign-on details or password.
- Students must abide by the rules in this document in respect of privately owned devices.
- The School has the right to confiscate any electronic device (personal or school owned) if they reasonably believe that it has been used to commit an offence, crime or breached the school rules in any way (please refer to Digital Safety policy 12.1)

Use of email and the internet

- Students must not search for, or display, any material considered illegal or offensive. A list of unacceptable and illegal material and related sanctions can be found in the table below;
- Students must not undertake any deliberate act with the intent of avoiding network security procedures.
- Students may only use appropriately named email accounts on the school system;.
- **Students must only use school email for communicating with members of staff;**
- Students should immediately tell a teacher if they receive an offensive email and should not respond to the email;
- Students should not reveal personal details of themselves or others in email communication, or arrange to meet anyone met online without specific permission;
- School email should only be used for work/educational purposes; it should not be used for personal messages during the School Day;
- Any email sent to an external organisation on behalf of the school should be written carefully and authorised by a teacher before sending;
- The forwarding of chain letters and the sending of offensive or inappropriate emails is not permitted;
- Publishing anything to the internet at school or elsewhere which causes offence or brings the school into disrepute may lead to disciplinary action;
- Students must have suitable anti-virus software installed on their private **DIGITAL TECHNOLOGY** equipment;
- The use of peer-to-peer programs is strictly forbidden on the school network and may lead to disciplinary action;
- Uploading of any media to a public site must be authorised by a member of staff;
- Video streaming/downloading is permitted providing no copyright has been infringed and it is legal to do so;
- The use of social media is permitted, however students should not post anything related to the School without authorisation from a member of staff.

Other use of digital technology

- Mobile phones and camera phones will not be used in the classroom, unless permission is given by the teacher.
- Video conferencing will only be used in lessons, with the teacher's permission during the school day.
- Only MP3 and image files connected with student work will be stored on the network.
- The use of cellular data (e.g. GPRS, EDGE, 3G, 4G, etc.) to access the Internet in
  School is discouraged and the school Wi-Fi should be used; if however students do access the internet in this way in school they agree to abide by this Acceptable Use Policy.
  Staff will only communicate with students via text or mobile phone when strictly necessary – for example whilst on a school trip. At such times, a mobile phone allocated for excursions will usually be used. Any student data including personal numbers will be deleted the conclusion of the trip.

The School will exercise its right to monitor the use of the School's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the School's information systems may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Unsuitable / inappropriate digital activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that students, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

Student Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**				X	X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.				X	X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008				X	X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986				X	X
	Extremism websites The Prevent Duty guidance March 2015 , Arising from the Counter terrorism & Security act 2015				X	X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	
	Any other information which may be offensive to students or staff or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
Online gaming (educational)			✓			
Online gaming (non educational)			✓			
Online gambling					X	
Online shopping / commerce			✓			
File sharing			✓			
Use of social media			✓			
Use of messaging apps			✓			
Use of video broadcasting e.g. YouTube				✓		

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures. The following table is a guide to what may happen:

Students	**Actions / Sanctions**								
Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year	Refer to Headmaster	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Recorded	Further sanction e.g. detention / Minor
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				X	
Unauthorised use of non-educational sites during lessons	X							X	
Unauthorised use of mobile phone / digital camera / other mobile device	X	X						X	X
Unauthorised use of social media / messaging apps / personal email	X	X						X	X
Unauthorised downloading or uploading of files		X				X		X	X
Allowing others to access school / network by sharing username and passwords					X			X	X
Attempting to access or accessing the school / network, using another student's / pupil's account					X			X	X
Attempting to access or accessing the school / network, using the account of a member of staff		X			X			X	X
Corrupting or destroying the data of other users		X						X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X			X		X	X
Continued infringements of the above, following previous warnings or sanctions			X			X	X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X	X			X	X	X	X
Using proxy sites or other means to subvert the school's / 's filtering system		X						X	X
Accidentally accessing offensive, pornographic or extremist material and failing to report the incident	X	X						X	
Deliberately accessing or trying to access offensive, pornographic or extremist material		X	X	X	X	X	X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X							X	X

As a user of school DIGITAL TECHNOLOGY equipment I have read and understood the above Acceptable Use Policy (AUP).

Student Name ……. Signed ……..

Parent name ……..Signed……

Tutor Group …….. Tutor…….. Date ……