Sidcot Acceptable Use Policy (Staff)

Sidcot School Digital Technology Acceptable Use Policy (AUP)

Sidcot School believes that effective use of Digital Technology is essential to enhance teaching and learning across the curriculum. Excellent use of Digital Technology allows teaching staff to:

- Teach in an effective way
- Utilise the power of multimedia and interactivity to teach and motivate
- 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
- Address some additional educational needs.

Information technology also provides an invaluable tool for all non-teaching staff to complete their functions within the school through:

- The financial management of the School
- The interchange of information within the School and with outside agencies
- The maintenance of records
- Ordering of materials, equipment and services.

However, there are potential dangers for students and staff. This policy has been written to ensure that Digital Technology is used effectively whilst minimising risk. 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 staff must complete this form and return it to the school. By signing this agreement staff agree to abide by its rules. Should any of these rules be broken or there be any other cause for concern the school will take appropriate action. Where necessary the police and/or other authorities will be informed.

To ensure that this policy is being followed, the school reserves the right to monitor the use of school systems, email and internet usage. All files / email and use of computers may be monitored and logged at Sidcot School and privacy should not therefore be assumed.

Use of Equipment

- Staff are expected to treat Digital Technology equipment carefully and not act in any way that might cause damage.
- Staff are to use school equipment for work purposes during the school day.
- Staff are to report any faults or damage found with school equipment to itsupport@sidcot.org.uk using your.name@sidcot.org.uk school email address.
- Owners of privately own devices must also abide by the rules in this document.

Use of Email and Internet

- Staff must check their school email at least once a day on a working day, for new messages when possible;
- When sending emails, the subject should not use anyone's name instead a generic title should be used;
- Staff must not search for, or display, any material considered illegal or offensive;
- Staff must not undertake any deliberate act with the intent of avoiding network security procedures;
- Staff may only use appropriately named email accounts on the school system;
- Staff must immediately report, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication to the Designated Safeguarding Lead or the Head of IT Services;
- Staff **must only** communicate with students using their school email. Unless authorised to do so by the Head of IT Services E.g. Exam results, **Failure of students to make use of the school email will not be deemed sufficient for authorisation of sending to personal email address.**
- Staff should not reveal personal details of themselves or others in email communication
- School email should only be used for work/educational purposes; it should not be used for personal messages during the school day;
- Email sent to an external organisation on behalf of the School should be written carefully and checked 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 via social media which causes offence or brings the school into disrepute may lead to disciplinary action;
- Staff must have suitable anti-virus software installed on their private IT 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 SMT;
- Video streaming/downloading is only permitted if no copyright is infringed and it is legal to do so;
- The use of personal social media is permitted; however staff should not post anything related to the school without authorisation from a member of SMT. (See Staff Student Code Appendix 1).
- Staff must never add a current or former student under 21 years of age, to any of their social networking accounts without authorisation from a member of SMT. (See Staff Student Code Appendix 1).
- Photos of students cannot be used for external web sites or promotion, unless the permission of the parents has been obtained. (See Digital Safety Policy 12.1).
- If staff are planning any activity which might risk breaking the acceptable use policy (e.g. research into terrorism for a legitimate purpose) SMT must be informed beforehand.
- Any digital communication between staff and students or parents / carers (email, chat, Parent Portal etc.) must be professional in tone and content and must use the staff email account.

Other use of digital technology

- Mobile phones and camera phones should not be used in the classroom (unless required for multi factor authentication)
- Only video and image files connected with school work can be stored on the network.

Data Protection

- Any school data must be stored on the school system and NOT on portable storage e.g. a USB stick unless the USB is one of the school approved encrypted USB Sticks
- Staff must be familiar with and abide by the GDPR (General Data Protection Regulations) at all times.(Digital Security Policy 12.2)

IT Systems

- Staff cannot install their own software or hardware. All requests for new software/hardware **must** go through the Head of IT Services
- Staff passwords must conform to the Sidcot School Password policy and must not be given out to anyone else.
- The network cannot be used for gambling and/or political purposes or used to view inappropriate material.
- All files and emails on the school network are the property of the School. As such, system administrators and SMT have the right to access them if required.
- All network access, web browsing and mails on the school system may be logged and can be monitored to ensure that the terms of the Acceptable Use Policy has not been broken.

Texting / Mobile Phones

- 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 be used. Any student data including personal numbers must be deleted at 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 is believed that 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 activities

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

Staff 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 colleagues 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 eg Youtube				✓		

Actions & Sanctions

It is intended that incidents of misuse (listed below) will be dealt with through normal disciplinary procedures:

Staff

Incidents:	Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	All these can/will result in disciplinary action
Inappropriate personal use of the internet / social media / personal email	
Unauthorised downloading or uploading of files that contain personal data or unlicensed software	
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	
Careless use of personal data e.g. holding or transferring data in an insecure manner	
Deliberate actions to breach data protection or network security rules	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students /	
Actions which could compromise the staff member's professional standing	
Actions which could bring the school / into disrepute or breach the integrity of the ethos of the school	
Using proxy sites or other means to subvert the school's filtering system	
Accidentally accessing offensive or pornographic material and failing to report the incident	
Deliberately accessing or trying to access offensive or pornographic material	
Breaching copyright or licensing regulations	
Continued infringements of the above, following previous warnings or sanctions	

As a user of school Digital Technology equipment I have read and understood the above Acceptable Use Policy (AUP), the Digital Safety Policy (12.1) and the Digital Security Policy 12.2

Staff member's name ……

Signed ……..…..…

Appointment …… Date: ……..…..…….……......

Document Change History

June 2024	Minor wording amendments
June 2025	Minor wording amendments