Online safety Policy

St. Paul's Crompton Street
December 2021

Policy Governance

Development, Monitoring and Review of this Policy

Matters relating to this policy or cross school initiatives may be considered by: Headteacher, teacher, support staff, governor or technical staff.

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Governors:

- Governors are responsible for the approval of the Online safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safety) of members of the school community
- The Headteacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff

Network Manager

The Network Manager ensures that the school's ICT infrastructure is secure and is not open to misuse or malicious attack

- that the school meets the online safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority Online safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy

Teaching and Support Staff

are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Online safety Co-ordinator for investigation/action/sanction
- encrypted devices are allocated to teaching staff to ensure the safe storage of data and sensitive information (see GDPR policy)

Safeguarding Lead and Deputy

should be trained in online safety issues and be aware of the potential for serious child
Protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

(N.B. it is important to emphasise that these are child protection issues, not technical issues, simply that the technology provides additional means for child protection issues to develop.)

Students/pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy, which will be outlined to them before being given access to school systems.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

Parents/Carers

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature. Parents and carers will be responsible for:

- accessing the school ICT systems in accordance with the school Acceptable Use Policy.

- Parents are asked to give annual consent to the following (a copy of the full letter is on the school website under policies – photographic consent letter.)

  As part of our day to day life in school, we may take photographs of the children. We may use these images in our school's prospectus or in other printed publications that we produce, as well as on our website and twitter. We may also make video or webcam recordings for schoolto school conferences, monitoring or other educational use. From time to time, our school may be visited by the media who will take photographs or film footage of a visiting dignitary or other high profile event. Pupils will often appear in these images, which may appear in local or national newspapers, or on televised news programmes.

Community Users

Community Users and visitors to the school who require access to the school network will do so under the guidance of the Headteacher and senior leaders.

Online safety Education and Training

Education – students / pupils

Online safety education will be provided in the following ways:

- A planned online safety programme(half termly Project Evolve lessons and special days) will be provided as part of computing/PHSE/other lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school
- Key online safety messages will be reinforced as part of a planned programme of activities
- Students/pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff will receive online safety training as part of their induction programme and through safeguarding training√, ensuring that they fully understand the school online safety policy and Acceptable Use Policies.
- The government document Keeping Children Safe in Education is read by all staff annually and refers to online safety throughout.

Communication devices and methods

The following table shows the school's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff & other adults				Students/Pupils			
Communication method or device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
								
Mobile phones may be brought to school	✓					✓		
Use of mobile phones in lessons		✓						✓
Use of mobile phones in social time	✓							✓
Taking photos on personal mobile phones or other camera devices				√				✓
Use of personal email addresses in school, or on school network	✓							✓
Use of school email for personal emails	✓							√
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓

Use of social networking sites		✓						✓

 This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
Communication method or device	***Staff & other adults***	***Students/Pupils***
Mobile phones may be brought to school		*Children walking home on their own – phones to be left in office during school day*
Use of mobile phones in lessons	*A discretionary approach is advised.*	
Taking photos on personal mobile phones or other camera devices		
Use of school email for personal emails	*Common sense advised. Mailing lists etc discouraged.*	
Use of social networking sites	*Limited to break/lunch times*	

Unsuitable/inappropriate activities

The accessing of unsuitable, inappropriate or illegal material is prohibited. The school will operate in line with the safeguarding needs of our children; in line with our values and within the law in terms of how we use online devices.

Incident Management

Incidents (students/pupils):	Refer to class teacher	Refer to Head of Key Stage	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	√	√	√	√	√	√	√	√	√
Unauthorised use of non-educational sites during lessons	√	√	√		√	√	√		
Unauthorised use of mobile phone/digital camera / other handheld device	√	√	√						
Unauthorised use of social networking/ instant messaging/personal email	√	√	√		√	√	√		
Unauthorised downloading or uploading of files	√	√	√		√				
Allowing others to access school network by sharing username and passwords	√	√	√		√	√	√		
Attempting to access or accessing the school network, using another student's/pupil's account	√	√	√		√	√	√		
Attempting to access or accessing the school network, using the account of a member of staff	√	√	√		√	√	√	√	√
Corrupting or destroying the data of other users	√	√	√		√	√	√	√	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	√	√	√	√	√	√	√	√	
Continued infringements of the above, following previous warnings or sanctions									√
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 pornography	√	√	√		√	√	√	√	√
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act			√	√	√	√	√	√	√

Incidents (staff and community users):	Refer to Head of Key Stage	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Removal of network / internet access rights	Warning	Further sanction *(please state)*
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	√	√	√	√	√	√	√
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		√				√	
Unauthorised downloading or uploading of files				√	√		
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 eg 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 instant 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 / pupils		√		√		√	
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							√

Further information and support:

The policy should be read alongside our policies and procedures including:

DFE: Keeping children safe in education Statutory guidance for schools and colleges

School Safeguarding and Child Protection Policy

School Staff Handbook

School Acceptable use policy

Appendix 1 – Student/Pupil AUP

Student/pupil Acceptable Use Policy Agreement Template

Student/Pupil Acceptable Use Policy Agreement
This Acceptable Use Policy is intended to make sure:

- That you will be a responsible user and stay safe while using the internet and other technology for learning and personal use
- That ICT systems and users are protected from accidental or deliberate misuse

The school will try to ensure that you will have good access to ICT to enhance your learning and will, in return, expect you to agree to be a responsible user.

Please make sure you read and understand the following ☑ **I WILL** and ☒ **I WILL NOT** statements. If there's anything you're not sure of, ask your teacher.

☑ I WILL:

- treat my username and password like my toothbrush – I will not share it, or try to use any other person's username and password
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- respect others' work and property and will not access, copy, remove or change any one else's files, without their knowledge and permission
- be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- immediately report any damage or faults involving equipment or software, however this may have happened
- only use internet sites that we are given permission to use and at the times that are allowed
* only complete searches related to work being completed

☒ I WILL NOT:

- try (unless I have permission) to make downloads or uploads from the Internet
- take or share images (pictures and videos) of anyone without their permission
- use the school ICT systems for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials
- open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes
- attempt to install programmes of any type on a machine, or store programmes on a computer
- try to alter computer settings
* share images on social media wearing uniform linking me to school