Willow Tree Primary School – E Safety and Mobile Technologies Policy

Introduction

Willow Tree will consider all current and relevant issues, in a whole school context, linking with other relevant policies, such as the Child Protection, Behaviour and Anti- Bullying policies.

The School E-Safety 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

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including e-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 e-safety allegation being made against a member of staff

E-Safety Coordinator/Officer:

- leads the e-safety committee and/or cross-school initiative on e-safety
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provides training and advice for staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- reports regularly to Senior Leadership Team

Network Manager / Technical staff:

The Managed Service provider is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority E-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 e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problems to the E-Safety Co-ordinator, Headteacher/ ICT Subject Leader for investigation/action/sanction

Designated person for child protection/Child Protection Officer

should be trained in e-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

School Achievement Committee

Members of the E-safety Committee (or other relevant group, e.g. Primary Schools may have a Safeguarding Committee, and this could be included as part of their remit) will assist the E-Safety Coordinator/Officer *(or other relevant person)* with:

- the production, review and monitoring of the school e-safety policy (Schools will need to decide the membership of the e-safety committee, which may include students/parents)

Students/pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (nb. At KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- 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/Learning Platform and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy
- accessing the school ICT systems or Learning Platform in accordance with the School Acceptable Use Policy.

Community Users

Community Users who access school ICT systems or Learning Platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

E-Safety Education and Training

E-Safety education will be provided in the following ways:

A planned e-safety programme will be provided as part of ICT and PSHCE lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school

- Key e-safety messages will be reinforced as part of a planned programme of assemblies
- 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 e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff will receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies

Communication devices and methods

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

	Staff & other adults				Students/Pupils			
Communication devices and methods	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 hand held devices eg PDAs, PSPs	☑					⚠		
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				☒				☒
Use of blogs				☒				☒

 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	Staff are provided with lockers. Mobile phones are to be locked in these during lesson time.	Children who walk to school/ home on their own can bring phones to school so long as they are handed over to the teacher's as soon as they arrive at school and take them only at home time. An agreement has to be signed.
Use of mobile phones in lessons		
Use of mobile phones in social time	During breaks or after school mobile phones may be used.	
Taking photos on personal mobile phones or other camera devices	Staff are not permitted to use their mobile phones to take photographs and/ or videos. School cameras IPAds should be used for this purpose.	
Use of personal hand held devices eg PDAs, PSPs		
Use of personal email addresses in school, or on school network	During breaks or after school	
Use of school email for personal emails		
Use of chat rooms / facilities		
Use of instant messaging		
Use of social networking sites		
Use of blogs	School Blog only	School blog only under supervision of an adult

Unsuitable/inappropriate activities

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

Unsuitable / Inappropriate Actions	Acceptable	Acceptable at certain times	Acceptable for Staff users	Unacceptable	Unacceptable and illegal
User Actions	☑			☒	☒
child sexual abuse images					☒
promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					☒
adult material that potentially breaches the Obscene Publications Act in the UK					☒
criminally racist material in UK					☒
Extremist or Terrorism related material					
Pornography					☒
promotion of any kind of discrimination					☒
promotion of racial or religious hatred					☒
threatening behaviour, including promotion of physical violence or mental harm					☒
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				☒	
Using school systems to run a private business				☒	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and / or the school				☒	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				☒	

Revealing or publicising confidential or proprietary information (eg. financial / personal information, databases, computer / network access codes and passwords)				☒	
Creating or propagating computer viruses or other harmful files				☒	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				☒	
On-line gaming (educational)				☒	
On-line gaming (non educational)				☒	
On-line gambling				☒	
On-line shopping / commerce		⚠	⚠		
File sharing				☒	
Use of social networking sites				☒	
Use of video broadcasting eg Youtube (No UPLOADING)			⚠		
Accessing the internet for personal or social use (e.g. online shopping)		⚠	⚠		
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses			⚠		

Good Practice Guidelines

Email

Best practice

☑ **DO**

Staff and students/pupils should only use their school email account to communicate with each other

Safe practice

Check the school e-safety policy regarding use of your school email or the internet for personal use e.g. shopping

Poor practice

☒ **DO NOT**

Staff: Do not use your personal email account to communicate with students/pupils and their families without a manager's knowledge or permission – and in accordance with the e-safety policy.

Images, photos and videos

Best practice

☑ **DO**

Only use school equipment for taking pictures and videos.

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Poor practice

☒ DO NOT

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.

Internet

Best practice

☑ DO

Understand how to search safely online and how to report inappropriate content.

Safe practice

Staff and students/pupils should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

☒ DO NOT

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Mobile phones

Best practice

☑ DO

Staff: If you need to use a mobile phone while on school business (trips etc), the school will provide equipment for you.

Make sure you know about inbuilt software/ facilities and switch off if appropriate.

Safe practice

Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first

Poor practice

☒ DO NOT

Staff: Don't use your own phone without the Headteacher/SLT knowledge or permission.

Don't retain service student/pupil/parental contact details for your personal use.

Social networking (e.g. Facebook/ Twitter)

Best practice

☑ **DO**

If you have a personal account, regularly check all settings and make sure your security settings are not open access.

Ask family and friends not to post tagged images of you on their open access profiles.

Safe practice

Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

Poor practice

☒ **DO NOT**

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.

Staff:

- Don't accept students/pupils or their parents as friends on your personal profile.
- Don't accept ex-students/pupils users as friends.
- Don't write inappropriate or indiscrete posts about colleagues, students/pupils or their parents.

Webcams

Best practice

☑ **DO**

Make sure you know about inbuilt software/ facilities and switch off when not in use.

Safe practice

Check the e-safety policy for any instances where using personal devices may be allowed.

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the school network immediately after the event.

Poor practice

☒ **DO NOT**

Don't download images from organisation equipment to your own equipment.

Don't use your own equipment without Headteacher/SLT knowledge or permission – and in accordance with the e-safety policy.

Don't retain, copy or distribute images for your personal use.

Incident Management

Incidents (students/pupils): Y = yes O = optional, at discretion of headteacher	Refer to class teacher	Refer to Head of Department / Head of Year / other	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)	y		y	o	y	o	o	y	o
Unauthorised use of non-educational sites during lessons	y		o			o		y	
Unauthorised use of mobile phone/digital camera / other handheld device	y		y			y	o	y	y
Unauthorised use of social networking/ instant messaging/personal email	y		y		o	o	o	y	y
Unauthorised downloading or uploading of files	y		y		o	o	o	y	y
Allowing others to access school network by sharing username and passwords	y		y		y	o	o	y	o
Attempting to access or accessing the school network, using another student's/pupil's account	y		y		y	o	o	y	o
Attempting to access or accessing the school network, using the account of a member of staff	y		y		y	y	o	y	y
Corrupting or destroying the data of other users	y		y		y	o	o	y	o
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	y		y	o		y	o	y	y
Continued infringements of the above, following previous warnings or sanctions	y		y	y	y	y	y	y	y

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	y		y	o	o	o	o	y	o
Using proxy sites or other means to subvert the school's filtering system	y		y		y	o	o	y	o
Accidentally accessing offensive or pornographic material and failing to report the incident	y		y		y	o	o	y	o
Deliberately accessing or trying to access offensive or pornography	y		y	o	y	y	o	y	y
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	y		y	o	y	y	o	y	y

Incidents (staff and community users): Y = yes O = optional, at discretion of headteacher	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc	Removal of network / internet access rights	Warning	Disciplinary Action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		y	y	y	y	y	y
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		y	o	y	o	y	o
Unauthorised downloading or uploading of files		y	o	y	o	y	o
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		y		y	o	y	o
Careless use of personal data eg holding or transferring data in an insecure manner		y	o	y	o	y	o
Deliberate actions to breach data protection or network security rules		y	o	y	o	y	o
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		y	o	y	o	y	o
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		y	o	y	o	y	o
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils		y	o	y	o	y	y
Actions which could compromise the staff member's professional standing		y	o	y	o	y	o

Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		y	o	y	o	y	o
Using proxy sites or other means to subvert the school's filtering system		y	o	y	o	y	o
Accidentally accessing offensive or pornographic material and failing to report the incident		y		y	o	y	o
Deliberately accessing or trying to access offensive or pornographic material		y	o	y	o	y	y
Breaching copyright or licensing regulations		y	o	y	o	y	o
Continued infringements of the above, following previous warnings or sanctions		y	o	y	y	y	y

Further Information and Support

For a glossary of terms used in this document:

http://www.salford.gov.uk/d/salford-esafety-glossary-jan2012.pdf

For e-Safety Practice Guidance for those who Work and Volunteer with, and have a Duty of Care to Safeguard Children and Young People:

http://www.salford.gov.uk/d/e-Safety-Practice-Guidance.pdf

R u cyber safe?

E-safety tips about how to stay safe online:

http://www.salford.gov.uk/rucybersafe.htm