

St Paul's CE Primary School E-Safety Policy

Review date: September 2024 Governor Approved Date: September 2024

Next Review: September 2025

Contents

Introduction
E-Safety Education and Training
Communication devices and methods
Unsuitable/inappropriate activities
Good practice guidelines
Incident Management
Further information and support
Appendix 1 - Student/Pupil AUP
••••••
Appendix 2 - Staff, Volunteer, Community User AUP
Appendix 3 - Use of Images Consent Form

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.

Policy Governance

Development, Monitoring and Review of this Policy

This e-safety policy has been developed by St Paul's governing body

Position	Name(s)	.9 2 2 3 7			
School E-Safety Coordinator / Officer	Mrs Katie Lavin				
Headteacher	Mrs Jane Tyers	Mrs Jane Tyers			
Governors	Executive Headteacher	Mrs. J. Tyers			
	Diocesan Representative	Rev. Daniel			
	Foundation Governor	Rev. M. Dyson			
	Chair	Mrs A. Darlington			
	Foundation Governor /Vice Chair	Mrs 5 Hughes			
	L.E.A. Governor				
	Staffing Governor	Mrs D Edwards			
	Community	Mrs Sue Darwin			
	L.E.A Governor	Cllr. A. Saunders			
	Co Opted	Miss S Casteldine			

Consultation with the whole school community has taken place through the following:

Forum	Date (if applicable)
Staff meetings	October 2021
Governors meeting	November 2021
Parents notification (dojo and website)	October 2021
School website	October 2021

Schedule for Review

This e-safety policy was approved by the Governing Body School Effectiveness Committee	November 2021
The implementation of this e-safety policy will be monitored by	Head teacher Deputy Head teacher E-Safety lead teacher Health & Safety, Buildings and Premises Committee
Monitoring will take place at regular intervals:	Every twelve months (Autumn 1) or sooner if needed
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group	Every twelve months
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	September 2025

Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager LA Safeguarding Officer
	Cathy Starbuck Police Commissioner's Office

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 e-safety of individuals and groups within the school:

Governors:

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

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including esafety) 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:

ICT Co-ordinator/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 problem for investigation/action/sanction
- to the:

```
i) E-Safety & ITLeader/Officer ii) Headteacheriii) Senior Leader iv) Classteacher
```

Designated person for child protection:

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

E-Safety Committee

Members of the Health & Safety, Buildings and Premises Committee will assist the E-Safety Leader/Officer, Mrs K Lavin, with:

the production, review and monitoring of the school e-safety policy

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
- 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

Education - students / pupils

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

- A planned e-safety programme will be provided as part of PHSE lessons using SCARF 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 and tutorial/pastoral 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 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 as part of the safeguarding package. An audit of the e-safety training (as part of safeguarding training) needs of all staff will be carried out regularly. It is expected that some staff will identify esafety as a training need within the performance management process.
- All new staff will receive e-safety training as part of their induction programme (safeguarding training), 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.

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			Stude				
Communication method or device	Allowed	Allowed at	Allowed for selected staff	Not allowed	Allowed	Allowed at	Allowed with staff nermission	Not allowed
	☑	<u> </u>	<u> </u>	28	☑	<u> </u>	<u> </u>	88
Mobile phones may be brought to school	☑						<u> </u>	
Use of mobile phones in lessons		<u> </u>						×
Use of mobile phones in social time	☑							×
Taking photos on personal mobile phones or other camera devices								<u> </u>
Use of personal hand held devices eg PDAs, PSPs				×				
Use of personal email addresses in school, or on school network		<u> </u>						2
Use of school email for personal emails		<u> </u>						×
Use of chat rooms / facilities				X				35
Use of instant messaging		<u> </u>		. a.				3
Use of social networking sites		<u> </u>			\(\frac{1}{2}\)			:

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		If child is walking home and needs to communicate with parents/carers.				
Lian of mobile phones in						
Use of mobile phones in lessons	For emergency appointments/phone calls and staff will leave the lesson if this occurs.					

During breaks/after school but not in the presence of children.	During breaks/after school but not in the presence of children.	
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	During breaks/after school when personal business has to be checked due to time constraints - but not in the presence of pupils.	

Use of school email for personal emails	During breaks/after school when personal business has to be checked due to time constraints - but not in the presence of pupils.	
Use of chat rooms / facilities		
Use of instant messaging	During breaks/after	
	school when personal business has to be checked due to time constraints - but not in the presence of pupils.	
Use of social networking sites		

a	part of a lesson dusing the school bsite blogs.	As part of a lesson and using the school website blogs.	
---	---	---	--

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:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illeaal
User Actions	☑	<u> </u>	<u> </u>	12	12
child sexual abuse images					2
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					æ
criminally racist material in UK				D	×
Pornography					*
promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					
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					
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					E
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	or breaches the integrity of the ethos of the school or			8	
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	Using school systems to run a private business			196	
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	that bypass the filtering or other safeguards employed by	3		Œ	
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	software or any copyrighted materials belonging to third	# # P		Œ	35
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the	information (eg financial / personal information, databases,			920	D 8
network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the		10 ±0		00	2
2 2 10 10 10 10 10 10 10 10 10 10 10 10 10	network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the			8	
On-line gaming (educational)	On-line gaming (educational)	9.	<u> </u>		
On-line gaming (non educational)	On-line gaming (non educational)			×	
On-line gambling	On-line gambling				

			×
On-line shopping / commerce	<u> </u>	<u> </u>	
File sharing	4		
Use of social networking sites			×
Use of video broadcasting eg Youtube			
Accessing the internet for personal or social use (e.g. online shopping)		<u> </u>	
Using external data storage devices (e.g. USB) that have			
not been encrypted (password protected and checked for viruses			

Good practice guidelines

Email





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

ur personal email account to communicate with students/p - permis manager's knowledge or saf sion – in accordance with the e ety policy.

Images, photos and videos





Only use school equipment for taking pictures and videos.

Ensure parental permission is in place.

Safe practice

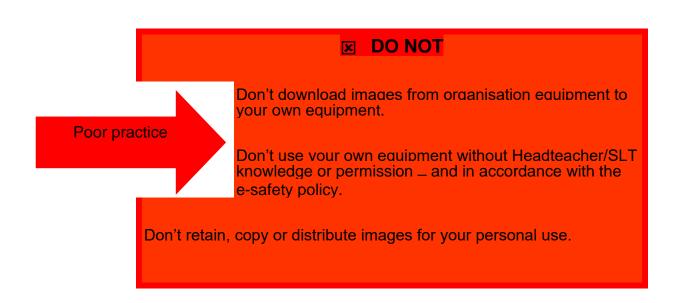


Check the e-safety policy for any instances where using personal devices may be allowed.

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.

Delete images from the camera/device after downloading.



Internet



☑ 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

Mobile phones Best practice Staff: If you need to use a mobile phone while on school business (trips etc.), the school will should provide

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

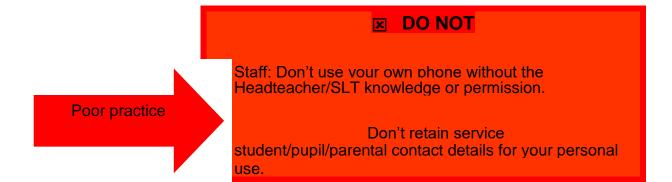
equipment for you.

Safe practice



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

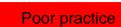
Staff: Make sure you know how to employ safety measures like concealing your number by dialling 141 first



Social Networking (e.g. Twitter/Facebook)



Safe practice





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

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



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

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

☑ 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 exstudents/pupils users as friends.
- Don't write inappropriate or indiscrete posts about colleagues, students/pupils or their parents.







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.

Delete images from the camera/device after downloading.

DO NOT

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

Poor practice

Don't use vour 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):	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 /	Removal of network / internet access riahts	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)			X	×	×	×	x		×
Unauthorised use of noneducational 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	×		×			×		X	×
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				x	×			x		
Accidentally accessing offensive or pornographic material and failing to report the incident				×		×		x		
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 Department / Head of	Year / other Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering /	Removal of network /	Internet access rights Warning	Further sanction	suspension whilst	incident is investigated
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	1000		×	×	×			×		
Excessive or inappropriate personal use of the internet / social networking sites / instar messaging / personal email	nt		×				×	×		
Unauthonicad daumlaadina			Х	х				×		
Unauthorised downloading or uploading of files	3									

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	x			×	×
Deliberate actions to breach data protection or network security rules	x	×			×
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	×	x		×	x
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	x			×	×
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	x	×	×	x	×
Accidentally accessing offensive or pornographic material and failing to report the incident	x		×	×	×

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

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

Appendix 1 - Student/Pupil AUP

Student/pupil Acceptable Use Policy Agreement Templat e

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: $\mathbf{\Lambda}$ 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 only use my personal handheld/external devices (mobile phones/USB devices etc) in school if I have permission 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

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, 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

Student / Pupil Acceptable Use Agreement Form Template

This form relates to the student/pupil Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I
 am involved in incidents of inappropriate behaviour, that are covered in this
 agreement, when I am out of school and where they involve my membership of
 the school community (examples would be cyber-bullying, use of images or
 personal information)
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I
 will be subject to disciplinary action. This may include loss of access to the
 school network/internet, suspensions, contact with parents and in the event
 of illegal activities involvement of the police

I have read and understand the above and agree to follow these guidelines when:

- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) eg mobile phones, PDAs, cameras etc
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, Learning Platform, website etc

(Parents/carers are requested to sign the permission form below to show your support of the school in this important aspect of the school's work).

Name of Student/Pupil	
Group/Class	
Signed (Student/Pupil)	Date
Signed (Parent/Carer)	Date

Appendix 2 - Staff, Volunteer, Community User AUP

Staff, Volunteer and Community User Acceptable Use Policy Agreement Template

.

School Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- that staff, volunteers and community users will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for students / pupils learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eq laptops, email, VLE etc) out of school.

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so
 with their permission and in accordance with the school's policy on the use of
 digital/video images. I will not use my personal equipment to record these
 images, unless I have permission to do so. Where these images are published
 (eg on the school website / VLE) it will not be possible to identify by name,
 or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

 When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules in line with the School's E-Safety Policy set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

- If I use my personal email address on the school ICT systems I will follow
 the rules set out in this agreement, in the same way as if I was using a school
 email. I will also follow any additional rules in line with the School's E-Safety
 Policy set by the school about such use.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not 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.
- I will not try (unless I have permission) to make large downloads or uploads
 that might take up internet capacity and prevent other users from being able
 to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/Local Authority Personal Data Policy where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student /
 pupil data to which I have access, will be kept private and confidential,
 except when it is deemed necessary that I am required by law or by school
 policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the student/pupil Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions in and out of school:

- I understand that this Acceptable Use Policy applies not only to my work and
 use of school ICT equipment in school, but also applies to my use of school
 ICT systems and equipment out of school and my use of personal equipment in
 school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy
 Agreement, I could be subject to disciplinary action. This could include a
 warning, a suspension, referral to Governors and/or the Local Authority and
 in the event of illegal activities the involvement of the police

· I have read and understood the School's E-safety Policy

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name	
Position	
Signed	
Date	