ONLINE SAFETY POLICY

The School Online Safety Policy applies to all members of the school community (including staff, 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. It is vital that all members of the school read and understand the policy and sign the relevant Acceptable Use Policies.

APRIL 2018

RATIFIED:
MAY 2018

REVIEW:
APRIL 2019

Contents

Introduction

This School Online Safety Policy has been produced by considering 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 Online Safety Policy applies to all members of the school community (including staff, 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.

It is vital that all members of the school read and understand the policy and sign the relevant Acceptable Use Policies.

Online Safety Policy

St Philip's CE Primary School
April 2018

St Philip's CE Primary School
Barrow St
Salford
M3 5LF

Policy Governance

Development, Monitoring and Review of this Policy

This Online Safety policy has been developed by a working group made up of:

Position	**Name(s)**
School Online Safety Coordinator	Katie Wright
Headteacher	Julia Kinch
ICT Technical staff	Tahir Iqbal
Governors	Jeremy Wisdom (parent governor)

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

Forum	**Date (if applicable)**
Staff meetings	25th April 2018
School / Student / Pupil Council	
INSET Day	4th June, 2018
Governors meeting	9th May, 2018
Parents evening	
School website / newsletters	

Schedule for Review

This Online Safety policy was approved by the *Governing Body on:*	*April 2018*
The implementation of this Online Safety policy will be monitored by: The Online Safety Working Group (see table above)	*Katie Wright* *Julia Kinch* *Jeremy Wisdom* *Tahir Iqbal*
Monitoring will take place at regular intervals:	*Termly by Sharif Patel* *Annually by the rest of the Online Safety Working Group*
The *Governing Body* will receive a report on the implementation of the Online Safety policy generated by the Online Safety Working Group at regular intervals:	*Once a year (April)*
The Online 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 Online Safety or incidents that have taken place. The next anticipated review date will be:	*April 2019*
Should serious Online Safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager* *LA Safeguarding Officer* *Police Commissioner's Office*

Scope of the Policy

This policy applies to all members of the school community (including staff, 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 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

Online Safety Coordinator/Officer:

leads the Online Safety committee and/or cross-school initiative on Online Safety

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

Network Manager / Technical staff:

RM and Salford LA are 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 Online Safety technical requirements outlined in 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). See Appendix 2.
- they report any suspected misuse or problem to the *Online Safety Co-ordinator* for investigation/action/sanction

The Designated person for child protection/Child Protection Officer 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

Pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy (see Appendix 1), which they will be expected to sign before being given access to school systems (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 Online 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 (see Appendix 2).

Online Safety Education and Training

Education –Pupils

Online Safety education will be provided in the following ways:

- A planned Online Safety programme will be provided as part of ICT/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 assemblies and tutorial/pastoral activities
- 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:

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

Education and Training – Parents and Governors

It is essential that Governors and parents receive Online Safety awareness and/or training and understand their responsibilities. Training will be offered as follows:

- *A planned programme of Online Safety awareness/ training will be made available to Governors and parents, through workshops and drop in sessions.*

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				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 or videos on personal mobile phones				☒				☒
Taking photos or videos on 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**	**Pupils**
Mobile phones may be brought to school		
Use of mobile phones in lessons		
Use of mobile phones in social time	*Before 8.30am, lunchtimes and after 3pm*	
Taking photos on personal mobile phones or other camera devices	On the school camera/iPad, but not on personal devices	On the school camera/iPad, but not on personal 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	For specific project work on a secured password-protected site	On a specific password-protected site for specific project work

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 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 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					
On-line gaming (educational)					
On-line gaming (non educational)					
On-line gambling					
Accessing the internet for personal or social use (e.g. online shopping, banking etc)					
File sharing e.g. music, films etc					
Use of social networking sites					
Use of video broadcasting eg Youtube					
Using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses)					

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

	Circumstances when these may be allowed	
User Actions	**Staff & other adults**	**Pupils**
On-line gaming (educational)	Part of a specific, supervised and time-limited project (e.g. MineCraft)	Part of a specific, supervised and time-limited project (e.g. MineCraft)
On-line gaming (non educational)		
On-line gambling		
Accessing the internet for personal or social use (e.g. online shopping, banking etc)	*Before 8.30am, lunchtimes and after 3pm*	
File sharing e.g. music, films etc		*e.g. only if copyright-free*
Use of social networking sites	Part of a specific, supervised and time-limited project (e.g. Twitter)	
Use of video broadcasting eg Youtube	*e.g. for showing educational videos*	
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 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: don't use your personal email account to communicate with 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.

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.

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

Delete images from the camera/device after downloading.

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 (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 / 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)			X						
Unauthorised use of non-educational sites during lessons		X	X						
Unauthorised use of mobile phone/digital camera / other handheld device	X								
Unauthorised use of social networking/ instant messaging/personal email		X	X						
Unauthorised downloading or uploading of files		X	X						
Allowing others to access school network by sharing username and passwords			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						
Corrupting or destroying the data of other users			X						
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature			X						

Continued infringements of the above, following previous warnings or sanctions			X	X					X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X						
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	X		X	X			
Deliberately accessing or trying to access offensive or pornography		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				

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 / security etc	Removal of network / internet access rights	Warning	Further sanction
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)		X	X	X			
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		X		X			
Unauthorised downloading or uploading of files		X		X			
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's		X	X	X			

account							
Careless use of personal data eg holding or transferring data in an insecure manner		X		X			
Deliberate actions to breach data protection or network security rules		X	X	X			
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		X	X	X			
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 pupils		X	X				
Actions which could compromise the staff member's professional standing		X	X				
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X					
Using proxy sites or other means to subvert the school's filtering system		X	X	X			
Accidentally accessing offensive or pornographic material and failing to report the incident		X	X	X			
Deliberately accessing or trying to access offensive or pornographic material		X	X	X			
Breaching copyright or licensing regulations		X	X	X			
Continued infringements of the above, following previous warnings or sanctions		X	X	X			

Appendix 1 –Pupil AUP

Foundation Stage AUP

Acceptable Use Policy – Foundation Stage

	I will look after school ICT equipment and tell a teacher straight away if something is broken or not working properly. I will log off or shut down a computer when a teacher tells me to.
	I will check with my teacher before printing.
	I will always keep myself safe and tell a teacher if something makes me worried or unhappy.
	I will only use the internet when an adult is with me. I will only go on websites that my teacher tells me to go on.

I understand that these rules help me to stay safe and I agree to follow them.

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

Key Stage 1 AUP

Acceptable Use Policy - Key Stage One

	I will use school computers for school work and not to upset or be rude to other people. I will ask my teacher for help if I can't work the computer I will look after the school's computers, laptops, cameras and iPads and tell a teacher straight away if something is broken or not working properly. I will log off or shut down a computer when I have finished using it.
	I will save only school work on the school computer and will check with my teacher before printing.
	I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy.
	I will only use the internet with permission from my teacher. I will only go on websites that my teacher tells me to. I will tell my teacher straight away if I go on a website by mistake. I will click on Hector when I see something I don't like. I will tell a teacher straight away if I see a website that is not my work. I will only login with my own username and password.

I understand that these rules help me to stay safe and I agree to follow them.

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

Key Stage 2 AUP

Key Stage 2 – Acceptable Use Policy

	I will only use my own username and password. I will always keep my passwords a secret. I will always keep my personal details private (My name, family information, journey to school, my pets and hobbies are all examples of personal details). I will not try to get past any security measures in place to protect the school network.
	I will only visit sites that are appropriate to my work at the time. I will tell a responsible adult if I see anything that makes me scared or uncomfortable when online.
	I will only use my school email account. I will make sure all emails I send are respectful. I will only open any email attachments when approved by an adult. I will only email or message people I know or those approved by a responsible adult.
	I will make sure all messages or comments I send are respectful. I will tell a responsible adult if I receive a nasty message or get sent anything that makes me uncomfortable when online. I will not reply to any nasty message or anything that makes me feel uncomfortable. I will only email or message people I know or those approved by a responsible adult. I will talk to a responsible adult before joining chat rooms or networking sites. I will never meet an online friend without taking a responsible adult that I know with me. I will always check with a responsible adult before I show photographs of myself.
	I will use ICT equipment safely and responsibly. I will only use school ICT equipment for my work. I will make sure all my work does not break copyright.
	I will not give my mobile phone number to anyone who is not a friend. I will always check with a responsible adult before I show any photographs of myself.

I WILL ALWAYS USE WHAT I HAVE LEARNED ABOUT E-SAFETY TO KEEP MYSELF SAFE ONLINE.

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

Pupil Acceptable Use Agreement Form

This form relates to the 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, detentions, 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) e.g. 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 Pupil		
Class		
Signed (Pupil)		Date
Signed (Parent/Carer)		Date

Appendix 2 – Staff, Volunteer, Community User AUP

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 *pupils* learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

Staff, Volunteer and Community User 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 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 Online 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 (e.g. 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 (see Staff Handbook P14)
- 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 (see Staff Handbook P14).
- I will only communicate with 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 Online 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.
- I will not use personal email addresses on the school ICT systems.
- 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 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 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 Online 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	

Appendix 3 – Use of Images Consent Form

Use of Digital / Video Images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may be using digital or video cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media, The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents are requested to sign the permission form below to allow the school to take and use images of their children.

Permission Form

Parent / Carers Name	
Pupil Name	

As the parent / carer of the above pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.

I agree that if I take digital or video images at, or of, school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed	
Date	