E-safety Policy

St Mark's CE Primary
Governing Body Approved: 14th March 2017
Review Date: March 2018

Policy Governance

Development, Monitoring and Review of this Policy

This e-safety policy has been developed by a working group made up of:

Position	Name(s)
School E-Safety Coordinator / Officer	Mr Damian Kay/Ms Donna Rawling
Headteacher	Mr Damian Kay
Teachers	Mrs Louise Mansfield
Support Staff	
ICT Technical staff	RM-Mark Royle
Governors	Mrs Claire Macpherson
Parents and Carers	Parent Council
Community users	N/A

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

Forum	Date (if applicable)
Staff meetings	*Termly*
School / Student / Pupil Council	*Safer Internet Day 2017*
INSET Day	
Governors meeting	*14th March 2017*
Parents evening	
School website / newsletters	

Schedule for Review

This e-safety policy was approved by the *Governing Body* on:	14th March 2017
The implementation of this e-safety policy will be monitored by:	*Safeguarding Lead/Child Protection Officer-Mr Damian Kay* *E-Safety Officer-Ms Donna Rawling* *Deputy Safeguarding -Mrs Louise Mansfield* *Senior Leadership Team*
Monitoring will take place at regular intervals:	*Termly*
The *Governing Body* will receive a report on the implementation of the e-safety policy generated at regular intervals:	*Yearly*
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:	*Summer 2017*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*Insert names / titles of relevant persons / agencies eg:* *LA Safeguarding Officer* *Police Commissioner's Office*

Scope of the Policy

We believe this policy relates to the following legislation:

- Obscene Publications Act 1959
- Children Act 1989
- Computer Misuse Act 1990
- Education Act 1996
- Education Act 1997
- Police Act 1997
- Data Protection Act 1998
- Human Rights Act 1998
- Standards and Framework Act 1998
- Freedom of Information Act 2000
- Education Act 2003
- Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Children and Young Persons Act 2008
- School Staffing (England) Regulations 2009
- Equality Act 2010
- Education Act 2011
- Protection of Freedoms Act 2012
- Counter Terrorism and Security Act 2015

The following documentation is also related to this policy:

- Dealing with Allegations of Abuse against Teachers and other Staff: Guidance for Local Authorities, Headteachers, School Staff, Governing Bodies and Proprietors of Independent Schools (DfE)
- Equality Act 2010: Advice for Schools (DfE)
- Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges (DfE)
- Prevent Strategy (HM Gov)
- Teaching approaches that help build resilience to extremism among people (DfE)
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children

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 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:

RM 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 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.

Internet Filtering and Use

RM provide the school with access to Smoothwall which allows us to manage a secure and filtered Internet service. The E-Safety Officer monitors Smoothwall on a daily basis and reports back to the Headteacher/SLT

Access to the Internet is designed to protect pupils and school personnel by blocking the following content:

☐ adult content containing sexually explicit images
☐ violent content containing graphically violent images
☐ hate material content promoting violence or attack on individuals or institutions on the basis of religious, racial or gender grounds
☐ illegal drug taking content relating to the use or promotion of illegal drugs or the misuse or prescription drugs
☐ criminal content relating to the promotion of criminal and other activities
☐ gambling content relating to the use of online gambling websites
☐ non educational websites such as social networking sites

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 to the *E-Safety Co-ordinator/Safeguarding lead/Child Protection Officer* for investigation/action/sanction

The 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

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 and information about national/local e-safety campaigns/literature. Parents and carers will be responsible for:

- endorsing the Student/Pupil Acceptable Use Policy
- accessing the school ICT systems in accordance with the school Acceptable Use Policy.

Community Users

Community Users who access school ICT systems 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 Computing 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 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:

- *All new staff will receive e-safety guidance 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.

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 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		*Phone may be needed for direct communication with parent/carer when travelling to/from from school. Therefore in such a situation the phone will be switched off and handed in at the office at 8.55am then collected at 3.30pm*
Use of mobile phones in lessons		
Use of mobile phones in social time	*e.g. during breaks or before/ after school but not within sight or sound of children*	
Taking photos on personal mobile phones or other camera devices	*If a member of staff is using the phone or other camera device to take photos for display purposes, as evidence of work or to record an activity/event/excursion. Photos must be uploaded to the school network asap then deleted from the phone immediately. Photos*	

	must only be printed using school facilities. No images should be stored on personal mobile devices for periods exceeding 24 hours.	
Use of personal hand held devices eg PDAs, PSPs		*PDA/PSP and IPAD/IPOD maybe allowed into school at certain times of the year e.g. end of term*
Use of personal email addresses in school, or on school network	*In case of school email not working and also in the case of awaiting the receipt of an urgent email. Use must be however during breaks or before/ after school and never within sight of children*	
Use of school email for personal emails		
Use of chat rooms / facilities		
Use of instant messaging		
Use of social networking sites		
Use of blogs	In the case of creating/ maintaining/using a school blog via the website/learning platform or using an appropriate website for teaching and learning and CPD (not social networking sites Facebook, Twitter)	Where children are supervised and guided in working on an online blog through the school website/learning platform or using an appropriate website in response to an issue e.g. bbc Newsround

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					☒
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		⚠			
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 communication 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 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.

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 and always within 24hrs

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 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 service student/pupil/parental contact details for your personal use.

Social networking (e.g. Facebook/ Twitter)

Schools should take into consideration the age of their pupils, and whether they are old enough to have accounts when including this guidance.

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 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.

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 (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 / 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		x		x	x	x		X
Unauthorised use of non-educational sites during lessons	x		x					X	
Unauthorised use of mobile phone/digital camera / other handheld device	x		x			x		X	
Unauthorised use of social networking/ instant messaging/personal email	x		x		x	x	x		
Unauthorised downloading or uploading of files	x		x		x	x	X		
Allowing others to access school network by sharing username and passwords	x				x			X	
Attempting to access or accessing the school network, using another student's/pupil's account	x		x		x	x	X		
Attempting to access or accessing the school network, using the account of a member of staff	x		x		x	x	x		X
Corrupting or destroying the data of other users	x		x		x	x	x		X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	x		x	x	x	x	x		X
Continued infringements of the above, following previous warnings or sanctions	x		x		x	x	x		x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	x		x		x	x	x		X
Using proxy sites or other means to subvert the school's filtering system	x		x		x	x	x		X
Accidentally accessing offensive or pornographic material and failing to	x		x		x	x		x	

report the incident									
Deliberately accessing or trying to access offensive or pornography	x		x	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	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	x		
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email		x		x	x	X	
Unauthorised downloading or uploading of files		x		x	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 account		x		x	x	X	
Careless use of personal data eg holding or transferring data in an insecure manner		x		x	x	X	
Deliberate actions to breach data protection or network security rules		x		x	x	X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x		x	x	x	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		x	x	x	x		X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with		x		x	x	x	

students / pupils							
Actions which could compromise the staff member's professional standing		x		x	x	X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x		x	x	X	
Using proxy sites or other means to subvert the school's filtering system		x		x	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 pornographic material		x	x	x	x		x
Breaching copyright or licensing regulations		x		x	x	X	
Continued infringements of the above, following previous warnings or sanctions		x		x	x		x

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 1a – Student/Pupil AUP

KS1 Student Acceptable Use Policy Agreement

Please make sure you listen carefully 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:

1/I will always follow the instructions of my teacher and not go on the internet without permission

2/ I will only look at or save pictures and text from the internet that are agreed by the teacher.

3/ I will tell an adult straight away if I see something on the computer or internet that I don’t like, or that upsets me in school

4/ I will tell my teacher straight away if anyone sends any upsetting messages to me on the computer at school.

5/I will always keep personal information like my name, address, phone number etc private

I WILL NOT:

1/I will not send any nasty messages to anyone online

2/I will not search for things on the internet that are unsuitable for my age

3/I will not give out mine or any other child’s details online

4/I will not click on pop ups or attempt to buy things online in school

5/I will not print anything online unless allowed by the teacher

Signed:

Appendix 1b – Student/Pupil AUP

KS2 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, 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 computing 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 via social media

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

Appendix 2-Staff Acceptable Use Policy Agreement

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

- Staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- School ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

- Staff 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 (eg 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 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 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.

- I will only use personal email addresses on the school ICT systems as highlighted in the allowance indicator on the grid found on p.13.

- 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).

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

Signed…………………………………........

Date………………………………………..

Appendix 3-Volunteer and Community User AUP

I understand that the school Internet facility is for the good of my professional development, for the development of this school and must be used only for educational purposes.

I realise that I have a personal responsibility to abide by the set rules and regulations when using the Internet and I am aware of the consequences if I breach them.

I am aware that by breaching the rules and regulations it may lead to:

- withdrawal of my user access
- the monitoring of how I use the Internet
- disciplinary action
- criminal prosecution

I will report immediately to the person responsible for any accidental access to inappropriate material or websites that I may have.

When using the school's Internet I will not:

- use the Internet in such a way that it will bring the school into disrepute
- use inappropriate or illegal websites
- download inappropriate material or unapproved software
- disrupt the time of other Internet users by misusing the Internet
- use inappropriate language
- use language that may provoke hatred against any ethnic, religious or other minority group
- produce, send out, exhibit or publish material that will cause offence to anyone
- divulge any personal information about myself, any other user or that of pupils
- use the login credentials or passwords of any other user
- use a computer that is logged on by another user
- use any social networking site inappropriately but only to use it in order to develop teaching and learning
- transfer the images of pupils without prior permission of the headteacher and from parents
- use email for private use but only for educational purposes
- compromise the Data Protection Act or the law of copyright in any way

Signed…………………………… Date…………………………….

Reason for visit

…………………………………………………………………………..........................

....

……………………………………………………………………………..

Appendix 4 – Use of Photographs/Videos parental consent form

Use of Photographs/Videos parental consent form.
Pupil Name(s):..
Class(es):...

I give permission to any photograph/video including my child/ren being used to promote and celebrate St Mark’s CE Primary School. I understand photos/videos may be used in school displays and presentations. I also consent to photos/videos of my child/ren *with no names attached* to be used online **(school website only)** and in social media **(school twitter only).**

Yes □

No □

Signed.............................   Print name/Relationship to child/ren...

Parents/Carers Agreement

St Mark’s CE Primary recognise that parents/carers take great pleasure in coming together as a school community for events such as Christmas plays, sports days and whole school celebrations. We understand parents/carers like to take photos or videos of their children as a keepsake or to share with family and are happy to grant permission for all parents/carers to undertake photography and videoing in such school events. However under our duty of care and in order to safeguard and respect the wishes of all parents/carers/children we ask that you read and sign the agreement below:

- I understand I must not publish photos/videos online, including on any social media sites or video sharing sites. Any such photos/videos published online may contravene Data Protection legislation.

- I understand that photos/videos must only be taken at the location of the event e:g the school hall, playground or field

Signed...

St Mark’s CE Primary recording and publishing

St Mark’s CE Primary School will on certain occasions have authorised staff/volunteers record and film events in order to later release on DVD for parents/carers. This recording will be in line with our Digital Images Policy that can be found on the school website and in line with all the information presented above in this document.

- I consent to the recording/publishing by authorised St Mark’s staff/volunteers Yes □ No □

Signed.............................   Print name/Relationship to child/ren...

PLEASE NOTE THAT WITHOUT THE SIGNING OF THIS PART OF THE CONSENT FORM THE RECORDING BY AUTHORISED STAFF/VOLUNTEERS FROM SCHOOL OF CHRISTMAS PLAYS AND END OF YEAR PRODUCTIONS FOR DVD CANNOT TAKE PLACE

This form is valid for the period of time your child/ren attend St Mark’s CE Primary.

Any area of signed consent in this form can be withdrawn by the parent/carer at any time by informing St Mark’s CE Primary School in writing.