St Charles RC Primary School

E-Safety Policy

2016-17

ST. CHARLES R.C.

PRIMARY

CHRIST IS AT THE CENTRE

C ompassionate

H elpful

R espectful

I nclusive

S haring

T ruthful

St Charles RC Primary School

E-Safety Policy

2016-17

Our mission at St. Charles RC Primary School is to try and centre our life in Jesus Christ, the spiritual foundation of our community.

We aim to pass on the faith we share in partnership with you.

We want the children in our care to grow and develop to their full potential within a caring Catholic community which recognises fully their true worth and God given talents. We look forward to working with you in a spirit of mutual trust and support.

We take pride belonging to St. Charles RC Primary School.

MISSION STATEMENT

As a family of God, we love to learn and learn to love

E Safety at St Charles RC Primary School

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in schools in recent years. Children and young people will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. There is a large body of evidence that recognises the benefits that ICT can bring to teaching and learning.

St Charles RC Primary School has made a significant investment both financially and physically to ensure many of these technologies are available to all our pupils. We perceive the benefits to outweigh the risks. However, we must, through our e-safety policy, ensure

that we meet the statutory obligations to ensure that children and young people are as safe as possible and are protected from potential harm, both within and outside school.
The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. Our school e-safety policy helps to ensure safe and appropriate use.

The use of these new technologies can put young children at risk. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individuals consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files

The potential for excessive use which may impact on the social and emotional development and learning of the young person.

As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

At St Charles RC Primary School safety is a part of the curriculum. Aspects of e safety are progressively taught in each year group.

The School E-Safety Policy

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. E-Safety Policy

The e-Safety policy is part of the School Development Plan and relates to other policies including those for ICT, anti-bullying and safeguarding. Mrs Rachel Coussons is the school's e-Safety coordinator who will work in collaboration with the child protection coordinator Mrs Clare Campbell (Head teacher).

Our e-Safety policy has been written by the school, building on the Salford e-Safety Policy template. It has been agreed by senior management and approved by governors The e-Safety policy and its implementation will be reviewed annually or in response to an incident.

School E-Safety Coordinator: Mrs R Coussons

Headteacher: Mrs Clare Campbell

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

Staff meeting: 03/10/2016

SLT meeting: 05/10/16

Governors meeting: 11/11/16

Curriculum and Premises Committee: 18/10/16

School website / newsletters On- going and regular E-Safety Policy

Schedule for Review

This e-safety policy was approved by the Governing Body on: 11/11/16

Effectiveness

The implementation of this e-safety policy will be monitored by: Mrs Rachel Coussons, E-Safety Coordinator Mrs Clare Campbell, Head teacher

Senior Leadership Team Monitoring will take place at regular intervals: At least once a year or in response to an incident.

The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group at regular intervals:

Annually 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 2017

Should serious e-safety incidents take place, the following external persons / agencies should be informed:

LA ICT Manager-Terry Walsh LA

Safeguarding Officer-Roisin Rafferty

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

The Managed Service provider is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the e-safety technical requirements outlined in the Salford City Council Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy

Teaching and Support Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)

- they report any suspected misuse or problem to the E-Safety Co-ordinator, class teacher or Headteacher for investigation/action/sanction Designated person for child protection/Child Protection Officer should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:
- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Students/pupils:

- are responsible for using the school ICT systems and mobile technologies in accordance with the Student / Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems (nb. at KS1 it would be expected that parents/carers would sign on behalf of the pupils)
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so Parents/Carers The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website/Learning Platform and information about national/local e-safety campaigns/literature.

Parents and carers will be responsible for:

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

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

E-Safety Education and Training Education

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

- A planned e-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 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 training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies
- Communication devices and methods

The following table shows the school's policy on the use of communication devices and methods. 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	X				X			
Use of mobile phones in lessons		X						X
Use of mobile phones in social time	X							X
Taking photos on personal mobile phones or other camera devices		X						X
Use of personal hand held devices		X					X	
Use of personal email addresses in school, or on school network		X						X
Use of school email for personal emails				X				X
Use of chat rooms / facilities				X				X
Use of instant messaging				X				X
Use of social networking sites				X				X
Use of blogs	X					X	X	

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

Communication method or device	**Staff and other adults**	**Students/Pupils**
Use of mobile phones in social time	During breaks or after school	Not allowed
Taking photos on personal mobile phones or other camera devices	Only if school device is unavailable. All photos must be uploaded and deleted from the device as soon as possible	Toy day, must ask permission of third party before taking any photographs
Use of personal hand held devices	When used as part of a lesson or during non-teaching time	On toy day or when used as part of a lesson
Use of personal email addresses in school, or on the school network	During school breaks or after school. Can be used if staff are having difficulties with their work email	Not allowed
Use of school email for personal emails	Not allowed	Not allowed
Use of chat rooms/facilities	Not allowed	Not allowed
Use of instant messaging	Not allowed on school network	Not allowed
Use of social networking sites	Not allowed on school network	Not allowed
Use of blogs	Blogs can be used by teaching staff	Pupils can use the school blog with permission under supervision of a member of staff. Staff must check posts before they are publisehd

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:

User Actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					X
Promotion or conduct of illegal acts, eg. Under the child protection, obscenity, computer misuse and fraud legislation					X
Adult material that potentially breaches the Obscene Publications Act in the UK					X
Criminally racist material in the UK					X
Pornography					X
Promotion of any kind of discrimination					X
Promotion of racial or religious hatred					X
Threatening behaviour including promotion of physical violence or mental harm					X

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				X	
Using school systems to run a private business				X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and or the school				X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				X	
Revealing or publicising confidential or proprietary information (eg financial/personal information, databases, computer/networking access codes or passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
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				X	
On-line gaming (educational)				X	
On-line gaming (non educational)				X	
On-line gambling				X	
On-line shopping				X	
File sharing				X	
Use of social networking sites				X	
Use of video broadcasting eg Youtube				X	
Accessing the internet for personal or social use				X	
Using external data storage devices eg USB that have not been encrypted (and checked for viruses)				X	

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. Poor practice Good practice guidelines Email E-Safety

Good practice guidelines – 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.
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. Poor practice Images, photos and videos

Good practice guidelines - 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.

Good practice guidelines – 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.

Good practice guidelines - Social networking

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.

Good practice guidelines – 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):

Incidents (students/pupils)	Refer to class teacher	Refer to Head teacher	Refer to Police	Refer to technical support staff for action	Inform parents / carers	Removal of network internet access rights	Warning	Further sanction detention /exclusion
Deliberately accessing or trying to access material that could be considered illegal	**X**	**X**			**X**		**X**	**X**
Unauthorised use of non educational sites during lessons	**X**						**X**	
Unauthorised use of mobile phone/digital camera / other handheld device	**X**	**X**					**X**	

Unauthorised use of social networking/ instant messaging/ personal email	X						X	
Unauthorised downloading or uploading of files	X	X		X			X	
Allowing others to access school network by sharing username and passwords	X	X		X			X	
Attempting to access or accessing the school network, using another student's/pupil's account	X	X		X			X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X		X			X	
Corrupting or destroying the data of other users	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
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	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	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X		X			X	

Incidents (staff and community users):

Incidents Staff	Refer to Head teacher	Refer to Police	Refer to technical support staff for action	Removal of network internet access rights	Warning	Further sanction disciplinary
Deliberately accessing or trying to access material that could be considered illegal	**X**	**X**			**X**	**X** **disciplinary**
Excessive or inappropriate use of the internet/ social networking sites/instant messaging/personal email	**X**				**X**	**X** **disciplinary**
Unauthorised downloading or uploading of files	**X**		**X**		**X**	
Allowing others to access school network by sharing username and passwords	**X**		**X**		**X**	**X** **disciplinary**
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**	**X** **disciplinary**
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	**X**		**X**		**X**	**X** **disciplinary**
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	**X**		**X**		**X**	**X** **Gross** **disciplinary**
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	**X**		**X**		**X**	**X** **disciplinary**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	**X**				**X**	**X** **disciplinary**
Actions which could compromise the staff member's professional	**X**		**X**		**X**	**X** **Gross**

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

E-safety tips about how to stay safe online: http://www.salford.gov.uk/rucybersafe.htm

Appendix 1

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. 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 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 (for example, cyber-bullying, use of images or personal information)
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I may have access to the school network/internet taken away from me, my parents might be informed and I will have to explain my actions to a member of the school leadership

team 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, handheld devices (such as Nintendo DS), 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 blog, 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:_____________________________ Class:__________________
Signed (Student/Pupil):_____________________________ Date:__________________
Signed (Parent/Carer):_____________________________ Date:__________________

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

I WILL:

- treat my username and password like my toothbrush – I will not share it, or try to use any other person's username and password
- immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- respect others' work and property and will not access, copy, remove or change any one else's files, without their knowledge and permission
- be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- 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, social networking, 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

Appendix 2 – Staff User Acceptable Use Policy Agreement

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.

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 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.
- I will only use personal email addresses on the school ICT systems under the circumstances set out in the School’s E-Safety policy.
- 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 I have specific permission to do so.
- 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:______________________________

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. Students/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 student / 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.

Sidned:____ Date:_____________________