St Joseph's Catholic Primary School

# Online Safety Policy

## Introduction

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. At St Josephs we realise what an essential tool the internet is as a resources to support both teaching and learning. The statutory curriculum requires pupils to learn to locate, retrieve and exchange information using ICT. Computer skills are vital for our children's life-long learning and employment. Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's online safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Safeguarding. The implementation of this online safety policy will be monitored at regular intervals. 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.

# Contents

**Appendices*:***



# 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, both in and out of school. It is impossible to remove all risk. However we will endeavour to build our pupils resilience and vigilance to the risks they may encounter when online, so that they have the confidence and skills to stay safe. Online safety is taught throughout the school in PHSE and computing lessons.

# Monitoring

This online safety policy is developed and then monitored by Mr T Findler with support from the school safeguarding team.

**Head teacher:** Mrs McFarlane

**Online Safety Responsibility**: Mr T Findler

**Online Safety Governor: TBC**

**Designated Safeguarding Lead**: Mrs P Harrand

**Date policy reviewed:** September 2022

The school will monitor the impact of this policy using:

- monitoring of pupil activity during lesson times
- logs of reported incidents our parent and pupils
- views regarding online safety

# Roles and Responsibilities

We believe that online safety is the responsibly of the whole school community. The following section outlines the roles and responsibilities 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. This will be carried out by the Governors receiving regular

information about online safety incidents and monitoring reports. A member of the Governing Body has taken on the role of online safety Governor.

The role of the online safety Governor will include:

- Regular meetings with the online safety Co-ordinator, Miss Hampsey
- Regular monitoring of online safety incident logs
- Reporting to relevant Governors committee / meeting

## Headteacher and Senior Leaders:

The Headteacher has overall responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the online Safety Co-ordinator Miss Hampsey

- The Headteacher / Senior Leaders are responsible for ensuring that the online safety Coordinator and other relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant.

- The Senior Leadership Team will receive regular monitoring reports from the online safety Co-ordinator.

- 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.

- The Head teacher has a role in ensuring all staff receives suitable professional development in order to teach other colleagues and pupils on how to stay safe.

## Online safety Coordinator:

- 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 all staff.

- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.

- Meets regularly with online Safety Governor to discuss current issues, review incident logs and filtering. Attends relevant meeting / committee of Governors.

- Reports regularly to Headteacher / Senior Leadership Team

## ICT Technician:

- To read, understand, contribute to and help promote the schools online safety policies.

- To read and understand and adhere to the school staff Acceptable Use Policy.

- To report any online safety related issues that come to your attention to the online safety coordinator.

- To develop and maintain an awareness of current online safety issues, legislation and guidance relevant to their work.

- To maintain a professional level of conduct in your personal use of technology at all times. To take responsibility for the security of the school ICT infrastructure and systems.

- Manage content filtering and follows information that the local authority gives as a guidance to maintain the school's systems and firewall.

- To ensure passwords are changed when necessary.

- Ensure software (including antivirus software) is regularly updated.

- Liaise with appropriate people and organisations on technical issues.

- Restrict all administrator level accounts appropriately.

- Ensure that access controls exist to protect personal and sensitive information held on school-owned devices.

- Ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.

## Teaching and Support Staff:

Teaching and support staff are responsible for ensuring that:

- they have read, understood and adhere to the schools Staff Acceptable Use and Social Media Policies.

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices.

- they report any suspected misuse or problem to the online Safety Coordinator / Headteacher / Senior Leader for investigation / action / sanction.

- online safety issues are embedded in all aspects of the curriculum and other school activities.

- pupils understand and follow the school online safety and rules established for acceptable use.

- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- they monitor ICT activity in lessons, extracurricular and extended school activities.

- they are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.

- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- to ensure that any digital communications with pupils should be on a professional level and only through school based systems, NEVER through personal mechanisms, e.g. personal email addresses, texts or mobile phones.

- staff must use school based ipads and cameras to take images and videos.

## Child Protection Co-ordinator

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:

- Read, understand, sign and adhere to the school pupil Acceptable Use Policy.
- To know and understand school policies regarding cyber bullying.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used outside school.

- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in school and at home.

- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school and at home, or if they know of someone who this is happening to.

- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be aware how to report an incident and that incidents maybe logged.

- To discuss online safety issues with family and friends in an open and honest way.

- To know and understand school policies on the use of mobile phones, digital cameras and hand held devices.

- Should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's online Safety Policy covers their actions out of school, if related to their membership of the school.

## Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parents' seminars, newsletters, letters, website and information about national / local online safety campaigns / literature.

Parents and carers will be responsible for:

- endorsing (by signature) the Pupil Acceptable Use Policy / Home school agreement.
- To help and support the school in promoting online safety.
- To discuss online safety concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology.

To consult with the school if they have any concerns about their children's use of technology.

### External Users and Guests

- The school will be sensitive and show empathy to internet-related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice where appropriate.

- Any external organisations will sign an Acceptable Use Policy prior to using any equipment or the internet within school.

- The school will provide an Acceptable Use Policy for any guest who needs to access the school computer system or internet on school grounds.

- The school will ensure that appropriate levels of supervision exist when external organisations make use of the internet and ICT equipment within school.

# Education

## Pupils:

Online safety education will be provided in the following ways:

- In accordance with the 2014 National Curriculum requirements, planned online safety teaching will be provided as part of Computing / PHSE /other curriculum areas (as relevant) and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. - Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should 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.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.

- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Rules for use of school computers / laptops / ipads / internet will be devised annually through discussion with pupils. These will be posted in classrooms and displayed on the Online Safety display board. Further guidance will be posted on ipad log-in screens.
- Staff should act as good role models in their use of ICT, the internet and mobile devices

## Parents / Carers

Although, it is recognised many parents and carers have only a limited understanding of online safety risks and issues, they undoubtedly play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. With this in mind, the school will therefore seek to provide information and awareness to parents and carers through:

- Letters and newsletters
- Parent workshops such as the Online safety Talk
- Reference to relevant online guidance provided by the school website or in paper format by the school office.

# Education & Training – Staff and Governors

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.

- All new staff receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and Acceptable Use Policies.

- This Online Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.

- The Online Safety Coordinator will provide advice / guidance / training as required to individuals as required.

- All staff will be trained in Safeguarding procedures, including elements of Online safety and The Prevent Duty.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

# Use of Digital and Video Images

When using images and video, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. It is vital both staff and pupils are aware of and take responsibility for their digital footprint. Images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, under no circumstances should the personal equipment of staff be used for such purposes.

- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the school's home school agreement (which seeks parental consent) on the use of images.

- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website or the school's social network accounts. An updated list will be kept by Mr T Findler online safety co-ordinator, the Headteacher and the school office. This list will also be given to all staff.

# Managing Internet Access and Security

Pupils will continue to use the Internet outside school and so will need to learn how to evaluate Internet information and that they need to take a responsibility of their online safety, behaviour and security. As a school it is our role to ensure pupils can balance the benefits of using the internet with an awareness of the potential risks.

## ICT System Security

- Users need to seek advice and permission from the school technical team before downloading any programs. An administration code is required.

- The school ICT systems capacity and security will be reviewed regularly by the schools ICT technical team.

- Virus protection is installed and updated regularly by the school technical team on all workstations within the infrastructure.

## Content Filtering

- The school's internet provision includes filtering appropriate to the age and maturity of our pupils.

The school will always be proactive regarding the nature of content which can be viewed through the school's internet provision.

- The school will have a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this procedure by reading and signing the Acceptable Use Policy.

- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the online safety Coordinator. All incidents should be documented.

- If users discover a website with potentially illegal content, this should be reported immediately to the online safety Coordinator. The school will report such incidents to appropriate agencies including the filtering provider. The school will regularly review the filtering product for its effectiveness.

- Any amendments to the school filtering or block-and-allow lists will be checked and assessed prior to being released or blocked through the school's technician, online safety coordinator or YHGfL. Pupils will be taught to assess content as their internet usage skills develop.

- Levels of internet access and supervision within our school may well vary depending on the user. Pupils and Teachers may have different filtering policies applied to their internet use, either temporarily or permanently as we have moved towards a less locked down service.

# Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

# Handling Incidents

Internet misuse will be dealt with and sanctions given by the class teacher at the time of the misuse.

Incidents will be reported to the online Safety Coordinator/ Child Protection Liaison Teacher / The Head Teacher who will judge whether it is necessary to just log the incident, or inform the Sheffield Safeguarding Team or/and the police.

If misuse is repeated, Parents will be informed.

Any complaint about staff misuse will be referred immediately to the Head Teacher and discussions with the local police if appropriate.

Complaints of a child protection nature must be dealt with in accordance with school child protection and safeguarding procedures.

Illegal issues with be handled through discussions with the Head Teacher, Child Protection Liaison Teacher, Governor Representative and Local Police.

# Emailing

- Pupils/staff must immediately tell a teacher/head teacher if they receive offensive or any unknown external e-mail within their own or group accounts.

- Pupils must not reveal personal details of themselves (including their e-mail address) or give information of other peoples details in e-mail communication, or arrange to meet anyone without specific permission.

- Any e-mail in school should only be sent through approved email accounts setup by the class teacher. Pupils must have permission before emailing in school. The passwords on these accounts can be changed by the teacher after the session if so required

# Social Networking Sites - Pupils

- Schools should block/filter access to social networking sites and newsgroups unless a specific use is approved.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
  Pupils should be advised not to place personal photos on any social network space.

- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Pupils are advised to only use moderated sites specifically for their age group and to seek consent from an adult.

# Social Networking Sites - Staff

When using digital communications, staff, students and volunteers should:

- only make contact with children for professional reasons and in accordance with the policies and professional guidance of the school.
- not share any personal information with a child e.g. should not give their personal contact details to children including e-mail, home or mobile telephone numbers.
- not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- not send or accept a friend request from the child/young person on social networks.
- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- ensure that all communications are transparent and open to scrutiny.
- be careful in their communications with children so as to avoid any possible misinterpretation.
- ensure that if they have a personal social networking profile, details are not shared with children in their care (making every effort to keep personal and professional online lives separate).

- not post information online that could bring the school into disrepute.

- be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

# Mobile Phone / Devices Usage in School

- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- Staff should not use mobile phones to take pictures or videos of children.

- Staff should only use digital cameras and ipads which have been provided by the school.

- Mobile phones are not permitted for use anywhere in school, around the children. This applies to members of staff and other visitors to the school.

- Mobile phones may only be used in office areas, staffroom etc. The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school, for use in emergencies only.

- Children who bring mobile phones to school are required to hand them in to the school office staff every morning and devices are collected at home time.

# The Prevent Duty and Online Safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well being of any pupil is being compromised.

# Protecting Personal Data

**(See Data Protection Policy for further Details)**

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
  Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

All staff in school must ensure:

- They take care and safe of all personal data, minimising the risk of its loss or misuse.

Use password protected computers and ensure equipment is logged-off at the end of the session where personal information could be accessed or viewed.

- Transfer or store data using encrypted and secure password devices.
- Any data transferred is used on a virus protected system which is regularly updated.
- All data is deleted from the device once transfer is complete.

Digital Cameras are cleared before allowing off site and photographs are transferred to the school protected systems.

- Equipment that is taken off site must be checked that no personal information can be accessed.

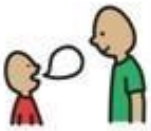
- All devices taken off site, e.g. laptops, tablets, removable media or phones, need to be secure in a locked, safe environment and, for example, not left in cars or insecure locations.

# Appendix A

## KS1 Internet Rules

THiNK Before You Click

These rules help us to stay safe when we use the internet.



We always ask an adult before we use the internet.

We only use websites and apps that our teacher has chosen.

We can click on the buttons and links when we know what they do.

We only search the internet with an adult.

We always tell an adult if we get lost on the internet or see something we don't expect.

# Appendix B

## KS2 Internet Rules

These rules help us to stay safe when we use the internet.

We ask permission before using the internet.

We only use websites and apps that an adult has chosen.

We tell an adult if we see anything we are uncomfortable with.

We immediately close any webpage we are not sure about.

We only email people an adult has approved.

We are polite and friendly on the internet.

We never give out our personal information or passwords.

We never arrange to meet anyone we don't know.

We do not open emails sent by anyone we don't know.

We do not use internet chat rooms or instant messaging without adult supervision.

We don't load images of ourselves or others without permission.

We use an alias name and avatar when online.

We know not to copy material from the internet as this is plagiarism.


# Appendix C

## Pupil Acceptable Use Policy Agreement – Key Stage 1

### This Acceptable Use Policy

We endeavour to teach our children to be responsible users of ICT and provide them with the guidance necessary to keep them safe when using online technologies. The school will try to ensure that our children will have good access to ICT to enhance their learning, but in return will expect the children to agree to be responsible users.

### This is how we stay safe at Key Stage 1 when we use computers:

- I will ask a teacher / an adult if I want to use the computer.
- I will only use activities that the teacher /an adult has told or allowed me to use.
- I will take care of the computer and other equipment.
- I will ask for help from the teacher / an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell the teacher / an adult if I see something that upsets me on the screen.
- I know not to talk to strangers online.
- I will keep my personal information and passwords safe.
- I will always be nice if I do post or put up messages online. I know that if I break the rules I might not be allowed to use the computer.

**Pupil Name:** _____ **Class:** _____

**Pupil's agreement**

I have read and I understand the School Rules for Acceptable Internet use. I will use the computer system and internet in a responsible way and follow these rules at all times.

Pupil signature: _____ Date: _____

**Parent's Consent for Internet Access**

I have read and understood the school rules for Acceptable Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: _____ Date: _____

**Please print name**: _____

# Appendix D

## Pupil Acceptable Use Policy Agreement – Key Stage 2

### This Acceptable Use Policy

We endeavour to teach our children to be responsible users of ICT and provide them with the guidance necessary to keep them safe when using online technologies. The school will try to ensure that our children will have good access to ICT to enhance their learning, but in return will expect the children to agree to be responsible users.

### Acceptable Use Policy Agreement

I understand that I must use the school's ICT resources in a responsible manner, to make sure that I keep myself and others safe whilst working online.

**Personal Safety**

- I will be aware of "stranger danger", when working online.
- I will not share personal information about myself or others when on-line.
- I will not upload any images of myself or of others without permission
- I will not arrange to meet up with people that I have communicated with online.
- I will immediately report any inappropriate material, messages I receive or anything that makes me feel uncomfortable when I see it online.
- I will report any bad behaviour by telling a responsible adult and will learn about using the CEOP Report button.
- I know that the school can look at my use of ICT and what I use online

**ICT Property and Equipment**

- I will respect all computer equipment and will report any damage or faults.
- I will respect others' work and will not access, copy, move or remove files.
- I will not use mobile phones/USB devices in school without permission.
- I will not use any programs or software without permission.
- I will not use or open email, unless I know and trust the person or organisation. • I will not install programs or alter any computer settings.

**Cyber Bullying**

- I will be polite when I communicate with others

• I know not to do online what I wouldn't do offline like in the playground
• I will not use inappropriate language or make unkind comments
• I appreciate others may have different opinions
• I will not upload or spread images of anyone

**The Internet**

• I understand that I need permission to be on the Internet.
• I will not fill in any online forms without adult permission
• I will not use any sites I've not had permission to use, this includes social media sites that I'm not old enough to use
• I will learn about copyright laws and make sure I acknowledge resources
• I will not upload or download images, music or videos without permission
• I will check that the information that I access on the internet is accurate, as I understand that the internet may not be truthful and may mislead me.

**Outside of the School Community**

• I understand that this agreement is for in and outside the school
• I know there will be consequences if I am involved in incidents of inappropriate behaviour covered in this agreement

---

Pupil Name: _____ Class: _____

## Pupil's agreement

I have read and I understand the School Rules for Acceptable Internet use. I will use the computer system and internet in a responsible way and follow these rules at all times.

Pupil signature: _____ Date: _____

## Parent's Consent for Internet Access

I have read and understood the school rules for Acceptable Internet use and give permission for my son / daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: _____ Date: _____

**Please print name**: _____

# Appendix E

## Acceptable Use Policy Agreement - Staff

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology 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 school digital technology and communications systems.
- 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- 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/ twitter) it will not be possible to identify by name, or other personal information, those who are featured.
- 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 mobile devices (laptops / tablets / 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 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 open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (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 Personal Data Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- 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).

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- The school advises that social networking and media sites are not used. If I do decide to use them, I will ensure that my personal use of these sites is compatible with my professional role and that privacy settings have been set. I am aware that sites are never fully private and that great care is needed when adding content.

- I will never undermine the school, its staff, parents or children. I know not to become "friends" with parents or pupils on social networks. I will always use my professional code of conduct if a parent relationship pre- existed and will never bring the school in disrepute.
- 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 / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

**I have read and understand the above and agree to use the school digital technology 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.**

**Staff / Volunteer Name:** .....

**Signed:** .....

**Date:** .....

# Appendix F

## Use of Digital / V ideo Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital 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.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

### Digital / Video Images 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. Yes / No

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. Yes / No

.....

Signed:

Date: .....

# Appendix G

Adapted from The Sheffield SafeGuarding Team - Staff Acceptable Use Policy Template 2012

# Record of Staff Training

| Staff Name | Online Saftey Training Attended | Code of conduct signed | Date |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

| | | | |
|---|---|---|---|
| | | | |