Catholic Umbrella Trust

E-SafeGuarding Policy

Acceptable Use Policies

Revised May 2016

(Version 9)

Adapted from Sheffield Safeguarding Children Board 2012

Contents

Appendices:

Policy Introduction

This E-SafeGuarding or E-Safety Policy is important to school for a number of reasons, including:

- To ensure we are aware of the e-safety issues that we face and teach e-safety to all members of the school community including pupils, parents, staff and governors
- To ensure there is a clear and consistent approach when responding to any incidents.
- To ensure that every person responsible for the children in our school is fully aware of their responsibilities.
- To set boundaries for the use of school owned technology, or personal equipment used in the school, and set the boundaries of services such as social networking platforms.

Rationale

The children in today's society have the opportunity to access a wide range of new technologies including the internet, a variety of communication technologies and other digital media. E-Safety encompasses both Internet technologies and electronic communications such as ipods, tablets and mobile phones. These are powerful and innovative tools which bring new opportunities for both teachers to teach and pupils to learn. Using such technologies promotes discussion, thinking, creativity, can stimulate learning and even raise educational standards and achievement. However, in order to use these technologies effectively, we need to educate our children about the benefits and risks they may encounter whilst online. These risks include:

- Cyber bullying
- Sharing, releasing and uploading personal information including images on websites and mobile devices
- Creating their own online profiles
- Using social media sites which can lead to grooming
- Accessing inappropriate images or content
- Predator danger when communicating or chatting with others online
- Distributing images without an individual's consent or knowledge
- Accessing violent games and videos
- Considering the reliability of information searched on the internet
- Plagiarism and copyright
- Illegal downloading of music and files
- Using a web cam

This e-safeguarding policy will be used in conjunction with other policies already embedded in school including the Behaviour, Anti-bullying, Safeguarding and Child Protection Policies. It is impossible to remove all risk. However, we will endeavour to build our pupils resilience to the risks they may encounter when online, so that they have the confidence and skills to stay safe.

E-Safety is taught throughout the school in PSHE and Computing lessons. (See E-Safety Framework for teaching coverage).

Development, Monitoring and Review

Title	**E-Safeguarding Policy**
Version	9
Date	*May 2016*
Author	*E-Safety Co-ordinator – Mrs Karen Sadler*
This e-safeguarding policy was approved by the Governing Body on*:*	Umbrella Trust Governors October 2013
The policy has been read and agreed by staff. Staff have signed the Code of Conduct	Each of the three schools are responsible for ensuring Staff have had a copy and have had adequate training/information.
Monitoring will take place at regular intervals (at least annually):	by Mrs K Sadler and Senior Leadership Teams
The Governing Body will receive a report on the implementation of the policy including anonymous details of any e-safeguarding incidents at regular intervals:	Every Term alongside the termly SafeGuarding Report
The 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:	*May 2017*
Should serious e-safeguarding incidents take place, the following persons / agencies should be informed:	*See Appendix B – Response to an incident of concern*

Monitoring

This e-safeguarding policy is developed and then monitored by Mrs Karen Sadler with support from the E-Safety Team on an annual basis or as a result of an incident taking place. The E-Safety Team includes as follows:

Roles	St Wilfrid's	St Thomas
Head Teacher	Mr P Scott	Mr L Colclough
Designated Safeguarding Lead	Mrs D Connolly	Miss O'Neil
Computing Coordinator	Mrs K Sadler	
ESafeGuarding Coordinators	Mr P Scott Mrs K Sadler	Mr L Colclough
SafeGuarding Governor	Maureen	
Designated Safeguarding Deputy	Mrs L McLoughlin (Learning Mentor)	

The school will monitor the impact of the policy using:

- Monitoring of pupil activity during lesson times
- Logs of reported incidents
- Our parents and pupils views regarding e-safety, whether through school council, questionnaires or workshops.

Awareness and training to deliver this policy will take place through the Curriculum, INSET Opportunities, Staff Meetings, Governor Meetings, Parent Workshops and through communication via the school's online community.

Communication of this Policy

- All amendments will be published and where appropriate awareness sessions will be held.
- Any eSafety updates will be included in the curriculum to ensure pupils are aware.
- ESafety training will be established across the school to include a regular review of updates within this policy.
- The key messages contained within the eSafeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed eSafeguarding messages across the curriculum whenever the internet or related technologies are used.
- Incidents will be dealt with, whether in or out of school in accordance with this policy, and other policies including Behaviour, Anti-bullying and Safeguarding. The school will, where known, inform parents of any incident which demonstrates inappropriate e-safety behaviour.

Senior Leadership

- The senior leadership team are responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school eSafeguarding policy and the use of any new technology within school.

Staff

- The eSafeguarding policy will be accessible to and discussed with all members of staff.
- The Staff Acceptable Use Policy Agreement will be discussed and signed.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.

Pupils

- Pupils together with their parent(s) need to read and agree to the Acceptable Use Agreement for Internet use in school. Parents need to approach the school if they disagree with any parts of the agreement.
- ESafety posters will be prominently displayed around the school.
- Teachers will reinforce the Pupil Acceptable Use Agreements through ICT lessons and will use the SMART rules within the curriculum.

Parents

- Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school online community.
- A Parents update at Curriculum evenings will be offered to highlight the dangers and provide useful information on how children can stay safe when using the internet.

Roles and Responsibilities

We believe that eSafeguarding is the responsibility of the whole school community, and everyone has a responsibility to ensure that all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Senior Leadership:

- The Headteacher has overall responsibility for esafeguarding all members of the school community, though the day to day responsibility for esafeguarding will be delegated to the Designated Safeguarding Lead Teacher.
- The Headteacher and senior leadership team are responsible for ensuring that the Designated Safeguarding Lead Teacher and other relevant staff receive suitable training to enable them to carry out their role and to train other colleagues when necessary.
- The senior leadership team will receive monitoring reports from the eSafeguarding Coordinator.
- The Headteacher and senior leadership team should ensure that they are aware of procedures to be followed in the event of a serious eSafeguarding incident. (see flow chart on *Appendix B – Response to an incident of concern* and relevant HR disciplinary procedures)

Governors:

- Approve and monitor the E-SafeGuarding Policy. Information will be given about all logged incidents.
- Read, understand, contribute to and help promote the school's eSafeguarding and Acceptable Use Policies.
- Develop an overview of the benefits and risks of the internet and common technologies used by pupils.
- Develop an overview of how the school ICT infrastructure provides safe access to the internet.
- Know how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the eSafeguarding Team in promoting and ensuring safe and responsible use of technology in and out of school.
- Ensure appropriate funding and resources are available for the school to implement its eSafeguarding strategy.

E-Safety Governor:

- Attends regular meetings with the E-Safety Co-ordinator
- Receives regular monitoring of e-safety incident logs
- Reports to Governing Body

Head Teacher:

- The Head Teacher is responsible for the safeguarding of all members of the school community.
- 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.
- The Head Teacher will act on any updates or monitoring which is needed and deals with any incidents appropriately.
- The Head Teacher and Designated Safeguarding Lead Teacher should be aware of procedures to be followed in an event of a serious incident or allegation being made with regards to e-safety.
- Monitors the recording of incidents within school.

E-Safety Team

- Ensures that the school eSafeguarding policy is current and systematically reviewed
- Ensures that school Acceptable Use Policies are appropriate for the intended audience.

- Promotes to all members of the school community the safe use of the internet and any technologies deployed within school.
- Ensures the school is aware of the procedures that need to take place in the event of any e-safety incident occurring in school.

Designated Safe Guarding Lead:

- Takes day-to-day responsibility for eSafeguarding within school.
- Has regular contact with other eSafeguarding committees including Sheffield Safeguarding Children Board
- Monitors any E-Safety incidents that have been recorded

Child Protection Officer:

- Understands the issues surrounding the sharing of personal or sensitive information.
- Understands the dangers regarding access to inappropriate online contact with adults and strangers.
- Is aware of potential or actual incidents involving grooming of young children.
- Is aware of and understand cyberbullying and the use of social media for this purpose.

E-Safety Coordinator:

- Promotes an awareness and commitment to eSafeguarding throughout the school.
- Takes a leading role in establishing and reviewing the school eSafeguarding policies and procedures.
- Leads the school eSafeguarding group or committee.
- Attends regular training to keep updated
- Reports to the Head Teacher any issues or incidents.
- Provides necessary training and support to staff.
- Liaises with other outside agencies when necessary, including the LA and Community Police.
- Communicates with school technical staff and with the designated eSafeguarding governor.
- Creates and maintains eSafeguarding policies and procedures.
- Develops an understanding of current eSafeguarding issues, guidance and appropriate legislation.
- Ensures that all members of staff receive an appropriate level of training
- Ensures that e-safety is embedded across the curriculum.
- Ensures that eSafeguarding is promoted to parents and carers.
- Monitors and reports on eSafeguarding issues to the eSafeguarding group and the senior leadership team as appropriate.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an eSafeguarding incident.
- Ensures that an eSafeguarding incident log is kept up to date.

Staff:

- Read, understand and help promote the school's eSafeguarding policies and guidance.
- Read, understand and adhere to the school Staff Acceptable Use and Social Media Policies.
- Report any incidents or misbehaviour with regards to e-safety to the e-safety coordinator
- Models safe and responsible behaviours in their own use of technology.
- 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.
- Implements the school e-safety policy and curriculum framework.
- Deliver e-safety objectives in all aspects of the school curriculum, including in antibullying week and Internet Safety Day
- Ensure the children understand and follow the Pupil Acceptable Use Policy
- Supervise ICT activities in school and ensure activities are focussed with clear pre-planned tasks to guide the children when on the internet
- Staff must use encrypted sticks for handling school data and school based digital cameras, devices and mobile phones for taking images and videos. Staff need to implement these rules on and off site.

- Create an environment where children know what to do if inappropriate material is discovered on the internet or if they feel threatened or uncomfortable with any form of online communication
- Ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- Ensure volunteers working alongside them adhere to the Visitor/Guest Acceptable Use Policy
- Understand and be aware of incident-reporting mechanisms that exist within the school.

Technical Staff:

- Read, understand, contribute to and help promote the school's eSafeguarding policies.
- Read, understand and adhere to the school staff Acceptable Use Policy.
- Report any eSafeguarding related issues that come to your attention to the eSafeguarding coordinator.
- Develop and maintain an awareness of current eSafeguarding issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in your personal use of technology at all times.
- Take responsibility for the security of the school ICT infrastructure and systems
- Manage content filtering and follows information that the Local Authority gives as guidance to maintain the school's systems and firewall
- Ensure passwords are secure and 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.

Protecting Our Staff, Students and Volunteers

Communication between adults and between children should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

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 eg 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.

Responsibilities of Pupils:

- To read, understand, sign and adhere to the school pupil Acceptable Use Policy.
- To know and understand the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policies regarding cyberbullying.
- 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 eSafeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents/Carers:

- To help and support the school in promoting eSafeguarding.
- To read, understand and promote the school pupil Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies. (Look at School E-Safety Blog and Newsletters)
- To discuss eSafeguarding 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.
- To read and sign the Parent/Carer Acceptable Use Policy form. **(If the form isn't returned back to school, this is the school's policy for Parent/Carers and it will be followed)**

Responsibilities of 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.

Educating School Members

Pupils

- Children will be continually encouraged during ICT sessions to think about e-safety and how to stay safe whenever online. The rules for acceptable use, which all pupils will have to sign, will be reinforced during these sessions.

- The E-Safety Framework is used as guidance to the appropriate activities and objectives the pupils should cover within ICT sessions on e-safety.
- E-Safety is also promoted through planned assemblies and during specific days and weeks like anti-bullying week and National Internet Safety Day. Activities will include using sites like the Think U Know website at www.thinkuknow.co.uk from the Child Exploitation and Online Protection Centre (CEOP) and the Childnet International site at http://www.childnet-int.org/.
- The SMART rules will be on display in each classroom and are reinforced during session time. A copy of these can be found in the Appendices.
- We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information and to consider the consequences their actions may have on others.
- Internet use is carefully planned and learners are guided to web sites which are age appropriate and support the learning objectives for specific areas of the curriculum.
- We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
- Children are taught what to do if inappropriate content is found during searches. Staff should be vigilant at all times when learners are searching.
- Learners are taught to be aware of the materials they access and to think about how to validate the accuracy of the information they find.
- Plagiarism and copyright laws are reinforced and the children are taught how to acknowledge materials used from the Internet.
- Pupils will be taught about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

All Staff and Governors

All staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff.
- An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies.
- This E-Safeguarding policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training as required to individuals as required.

Parents and 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 and in promoting the positive use of the internet and social media. The school will take every opportunity to help parents understand these issues through

- parents' / curriculum evenings
- newsletters
- letters
- website / e-safety blog

Using Digital and Video Images

(See Appendix I – Taking Photographs at School Events)

All members of the school community need to be aware of the risks associated with the sharing and posting of digital images on the Internet. The images used cannot be removed from the internet and so are there forever. This could be damaging and cause harm or embarrassment to individuals whether now or in the future years. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. Therefore it is important that we as educators take the following actions:

- Teach our members the risks associated with the taking, sharing and distribution of images. For example, on social networking sites, they are on view to potential employers (cyber vetting) and potential groomers. We need to teach all school members about their digital footprint and the risks attached with publishing their own images.

- Staff to plan the photographs they take for educational purposes and ensure pupils are appropriately dressed. We need to ensure we have parental consent to use or publish those images. Images should only be taken on school equipment, use of personal equipment needs to be authorised by the head teacher.

- Learners are taught not to upload, share or distribute images of themselves or others to the internet without seeking permission. Educational Videos like “Think Before You Post” (by CEOP) will be viewed to get this message across.

- Students’ / 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 students / pupils are published on the school website, prospectus etc. (see form in appendix)

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 works in partnership with YHGfL to ensure filtering systems are as effective as possible.
- 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 eSafeguarding Coordinator. All incidents should be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding 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, e-safeguarding 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.

Setting Passwords

- A secure username and password convention exists for all system access. The technicians can access all equipment including resetting users passwords when necessary.
- Key Stage 1 pupils will have a generic 'pupil' logon to all school ICT equipment.
- Pupils at Key Stage 2 are moving towards individually-named user account and password for access to ICT equipment.
- All staff will have a unique, individually-named user account and password for access to ICT equipment and information systems available within school.
- Users should change their passwords at prearranged intervals or at any time that they feel their password may have been compromised.

- All staff and pupils have a responsibility for the security of their username and password. Users must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. All personal passwords that have been disclosed should be changed as soon as possible.
- Never save system-based usernames and passwords within an internet browser.
- All access to school information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Users should create different passwords for different accounts and applications.
- Users should use 8 characters including numbers, letters and special characters in their passwords (! @ # $ % *)

Internet Access

- Pupils and Staff will discuss and sign the Acceptable Use Policy to know what Internet use is acceptable.
- When a member of the school community departs from the school the technical team must ensure any user information held by this member has been deleted to safe guard children and school data. This includes google accounts and access to the online community.
- Any visitors who are with the school for a period of time must also agree to the Acceptable Use Policy relevant to them.
- Parents will be informed that pupils will be provided with supervised Internet access and will be asked to read the Acceptable Use Policy with their child. If they disagree it is the parent's responsibility to inform the school. (This information will be included in all new pupils starter packs)

Internet Use

- Staff should guide pupils in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Handling Incidents – See *Response to an Incident of Concern* in Appendix B

- 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 E-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

- The School uses Yorkshire and Humber Grid for Learning Firewall which blocks/filters access to social media sites unless a specific use is approved as in Edmodo.
- Pupils are advised to only use moderated sites specifically for their age group and to seek consent from an adult.
- Pupils are advised never to give out personal details or complete online forms of any kind which may identify them or their location
- Pupils are advised not to upload personal photos of themselves or others on any social network space without permission.
- Pupils are advised on security and encouraged to set 'strong' passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils are encouraged to use privacy settings and invite known friends only and deny access to others if such sites were to be used.

Video Conferencing/ Skype

- Videoconferencing/skype will only be used in a teacher directed and supervised environment.
- Staff need to ensure the connection is closed after use.
- It will only be installed on teacher's main classroom computers.

Managing Emerging Technologies (Netbooks, Tablets, Cameras, Mobile Phones)

- Emerging technologies will be examined for educational benefit and a risk assessment will be discussed by the e-safety team before use in school is allowed.
- All equipment in school is to support the education and wellbeing of our children.
- Focussed tasks will be provided to the children when allowed on any of these emerging technologies and boundaries set by the teacher.

Mobile Phone / Devices Usage in School

- Mobile phones and other devices will not be used for personal use during formal school time.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
- Mobile phones are forbidden on trips unless consent has been given by a member of staff.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times in a bag.
- No images or videos should be taken on any mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- 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 have the right to confiscate and search pupil's devices if a safeguarding incident has been brought to their attention. Any evidence will be taken and stored appropriately.
- The sending of abusive or inappropriate messages is forbidden.
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office.
- If a pupil needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Pupils should protect their phone numbers by only giving them to trusted friends and family members. Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Google Education Apps
Staff Users

- At present only staff members of the school use google education apps for communication and sharing purposes.
- Staff use google email, calendars, documents and sites.
- No personal data relating to staff or pupils is placed on the application.
- Only initials or first names of the children are used
- There are no advertisements used with Google Apps for Education. Gmail offers web clips at the top of the inbox which show you news headlines, blog posts, RSS and Atom feeds. You can choose to Hide all advertisements from the control panel. Additional information on google security and filtering can be found at:
- http://www.google.com/support/a/bin/answer.py?answer=60762
- http://www.google.com/support/a/bin/answer.py?answer=60730

Online Community (See Website Policy)

- The school's online community is developed and updated by its school members who ensure that content is accurate, up to date and safe for public access.
- Contact details include the school address, e-mail and telephone number. Staff or pupils personal information will not be published without consent.
- It is a communication tool used for pupils, parents and staff of the school. The public can access the site to find out about the school and to share its successes.
- Blogs are an everyday part of the site and through e-safety training with our pupils and monitoring we ensure the blogs are safe to view.
- This online community helps us to prepare our children for the safe use of the internet when they are in and out of school.

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.
- They send personal data securely off the school site. (See School Business Manager)
- 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.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

List of Appendices

SMART Rules for Wall Display – **Appendix A**

Response to an Incident of Concern **– Appendix B**

Wall Display of Pupil E-Safety Rules– **Appendix C**

School Visitors and Whole School E-Safety Rules – **Appendix D**

Pupil Acceptable Use Agreement – **Appendix E**

Parent/Carer Acceptable Use Agreement– **Appendix F**

Staff Acceptable Use Policy Agreement – **Appendix G**

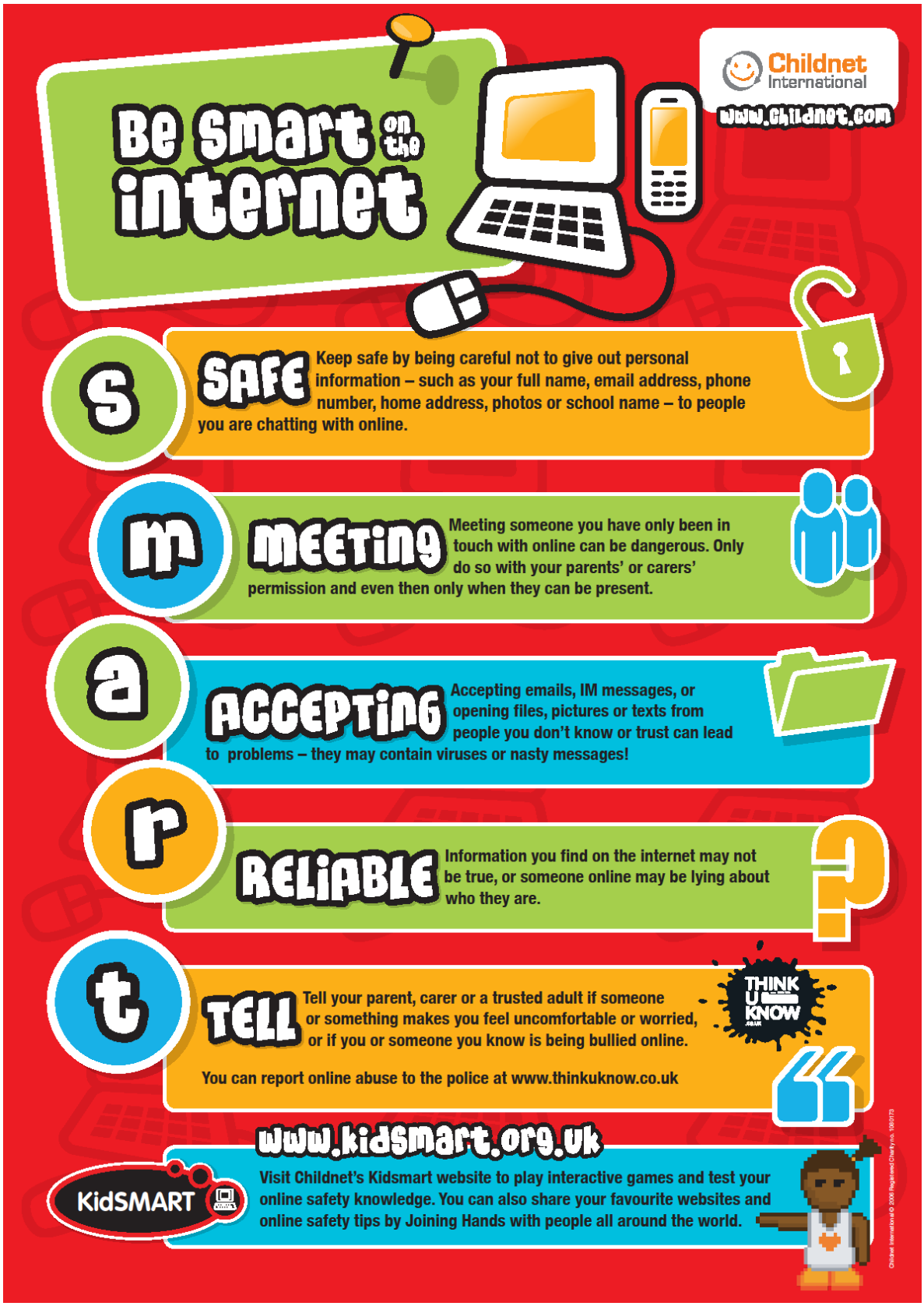
Online Incident Log Sheet – **Appendix H**

Taking Photographs at School Events – **Appendix I**

Photographs and Videos of Children – **Appendix J**

Organisations, Documents and Resources **– Appendix K**

Appendix A – SMART Rules to be on display



Appendix B - Response to an Incident of Concern

e-Safety Incident Occurs

If a child is at immediate risk
↓
Inform the Designated Child Protection Coordinator and follow school's child protection procedures
↓
Seek advice from Safeguarding Advisory Service
↓
Contact Sheffield Police (999) urgently if there is immediate danger

Contacts
- Sheffield Safeguarding Advisory Desk 0114 205 3535
- e-Safety Coordinator / Head
- Julia Codman 0114 293 6945
- Sheffield Police 0114 220 2020
- Child Exploitation and Online Protection Centre (CEOP) www.ceop.police.uk

Illegal Activity of Material found or suspected

- Content
  - Contact e-Safety Coordinator
  - Report to Filtering, Report to Internet Watch Foundation (www.iwf.org.uk) Or South Yorkshire Police
- Activity
  - Child
  - Staff
  - Contact Safeguarding Advisory Desk for advice
  - Report to CEOP www.ceop.police.uk
  - Child protection procedures and / or criminal action
  - Staff allegations procedures and / or criminal action

Unsure

- Consult with e-Safety Coordinator/ Team

Inappropriate Activity or Material

- Activity
  - Child
    - Possible School Actions:
      - Request support / advice from e-Safety Coordinator
      - Pupil Sanctions
      - PHSE/citizenship Sessions
      - Anti-Bullying
      - Parental Work
      - School support e.g. counselling, peer mentoring
  - Staff
    - Possible School Actions:
      - Head Teacher Involvement
      - Request support / advice from e-Safety Team
      - Staff Training
      - Disciplinary action
      - School support e.g. counselling,
- Content
  - Report to Filtering Manager and / or Schools Broadband Help Desk

Review Schools e-Safety policies and procedures, record actions in e-Safety Incident log and implement any changes for future

Contact Details

Schools Designated Child Protection Officer:
School e-Safety Coordinator:

Pupil Sanctions:

Reinforce the Acceptable Use Agreements and log incidents

Give appropriate sanction:
1. Warnings
2. No Internet Activity
3. Inform Head Teacher
4. Inform Parents

Appendix C – Key Stage 1 and Key Stage 2 E-Safety Rules

Early Years Internet Rules

Internet and computers are fun,
but we always ask a grown up before using one

Chatting and emailing is great,
but talking to strangers, NO WAIT!

This is my password and I must hide it away;
so that others can't use it another day.

It is always good to be polite;
we would never in school be unkind or fight.

Sharing with my friends can be fun;
but sharing on the internet should not be done.

Family and friends are those you know well;
strangers are those you don't meet or tell.

Using a nickname is the right thing to do;
sharing your information, just won't do!

Never be afraid to say something is wrong;
you are not on your own, so stay strong.

Later Years Internet Rules

Think Before You Click!

- We ask permission before using the Internet
- We stay focussed on the tasks set by the teacher
- We tell an adult if we see anything we are uncomfortable with.
- We immediately use Hector or close any sites we are not sure about.
- We only e-mail people an adult has approved.
- We do not open e-mails sent by anyone we don't know.
- We type messages that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don't know.
- We do not set up our own profiles without permission
- We do not enter chat rooms or use instant messaging without adult supervision
- We don't upload images of ourselves or others without permission
- We use an alias name and an avatar when online
- We only use our first name when blogging
- We never complete any forms online
- We acknowledge where we get our images from
- We know not to copy material from the internet as this is plagiarism

Appendix D: School Visitors E-Safeguarding AUP

These e-Safety Rules help us to protect pupils and the school community by describing acceptable and unacceptable internet and social media use as a visitor, student, guest or a member of staff in our school.

The School Computer Network

- The school owns the computer network and sets rules for its use. Therefore, it is a criminal offence to use the network for a purpose not permitted by the school.
- All network and Internet use must be appropriate to education.
- Irresponsible use may result in the loss of network, Internet access or even further action could be taken if misused.
- Network access must be made via an authorised account and password, which must not be given to any other person.
- The school IT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- Copyright and intellectual property rights must be respected.
- Messages and any online postings shall be written carefully and politely.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal any personal information.

Use of Personal Devices

- Personal devices like mobile phones or tablets are not to be used in classrooms, visits or during sporting activities to take images or videos of the children without permission from the class teacher or senior management.

Using Social Media

- Personal Social Media accounts are not accessed on the school's systems.
- Social networking sites should never be used for raising or escalating concerns about the school that may bring employees or the school into disrepute.
- Visitors must comply with the requirement to maintain child, parent, family and school employees confidentiality at all times and not to share any identifiable information online or through a social networking site.
- It is not permitted to use social networking sites as a forum for posting inappropriate comments about the school's employees, children, parents or families as a result from visiting the school.

Name: …… Signature: ……..Date:……

The school may exercise its right to monitor the use of the school's computer systems, including access to web-sites, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's computer system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

Pupil Acceptable Use Policy Agreement – Key Stage 2

This Acceptable Use Policy

We endeavor 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 keep my passwords safe and will not use other people's passwords
- 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 learn how to use the '***thinkuknow'*** web site to keep myself safe.
- 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.
- I will only use approved and moderated chatrooms or social networking sites with permission from a responsible adult

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.

Mobile Phones

- I know that mobile phones are not allowed to be used during the school day and are advised to be left at home.
- If consent has been given then mobile phones are switched off / silent and kept in my school bag or in the office at all times during the school day.
- Permission by the teacher will be given to me if I can use a mobile phone in school or take it on a school visit.
- I know not to use text, voice messages, take images or use any internet connection to bully, upset or shock anyone in and out of school.
- I know that no images or videos should be taken on any mobile phones or personally-owned mobile devices without the consent of the person or people it involves.
- I know that the school is not responsible for any loss or damage to my mobile phone or any device I bring onto the school site.
- I understand that the school have a right to confiscate, search and keep any evidence on any mobile devices I bring into school.
- I know that I should protect my phone number by only giving them to trusted friends and family.

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

All pupils need to sign these rules on the form provided and/or in class with a teacher at the start of each new academic year. This shows that they have read, understood and agree to the Pupil Acceptable Use Agreement.

Pupil Acceptable Use Policy Agreement – Key Stage 1

This Acceptable Use Policy

We endeavor 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.

Parent/Carer and Pupil Acceptable Use Policies Agreements

As part of the programme of activities in school, all pupils have the opportunity to access a wide range of communication technology resources. These resources are an essential part of promoting children's learning and development; however, we also recognise the potential risks associated with these technologies. We therefore have an E-Safeguarding and Acceptable Use Policies in place in school.

In recent years, social networking sites such as Facebook, Twitter, Instagram and Snapchat have grown in popularity and many people use them to communicate with family and friends. The vast majority of people who use social networking show respect in their communication with others and is something we must encourage to show our children that we are positive 'digital role models'. However, there are times when people disregard the rules and will use social networking sites to cyberbully and harass others.

There have been a number of high-profile cases in the media where people have used the internet to intimidate and bully others. The police have investigated these cases and in some instances have led to criminal prosecutions.

As a school, we encourage our parents to support us with the education and wellbeing of their children and if at any time, parents feel they have issues regarding their child's education, they should see their class teacher. If the issue has not been resolved then an appointment can be made with the Head teacher. We also have a complaints policy on the school website if deemed necessary.

As a community, we should all frown upon the use of social networking sites by parents to criticise and make unsubstantiated comments about the school or any members of staff.

We do not want to go down the line of sending out legal letters from solicitors to parents about untrue and damaging comments made on social networking sites. Current laws such as the 1988 Malicious Communication Act, 1997 Protection from Harassment Act and 2003 Communication Act can be used to protect people from damaging, malicious and threatening posts on the internet.

If an incident is reported to school staff, it should be investigated and, if school deem it appropriate, will be acted upon by the school's Head teacher and Safe Guarding Lead. In extreme cases, the Head teacher would consider whether it appropriate to notify the police or solicitors to take further action.

Therefore, as a Parent/Carer, you are asked to:

- Read the **Parent/Carers Acceptable Use Agreement**
- Read and talk to your child about their **Pupil Acceptable Use Agreement**
- Parent/Carer and child to **sign the agreement** on the enclosed form and **return to school**.

*(**NB** This is the school's policy for Parent/Carers and Pupil's Acceptable Use)*

If you disagree with any of the rules within the agreements or feel there is an area of Internet Safety you feel is not being developed please contact the Head teacher.

Please remember, all children in school are taught how to keep safe and be responsible when they are online, whether they are at school or at home. As children are able to access the internet outside school, whether this is at home, a friend's house or on a mobile device, we need to work in partnership with you the parent/carer to keep our children, staff and community safe.

Parent / Carer Acceptable Use Agreement:

- I have read and discussed the agreement with my child and confirm that he/she has understood what the rules mean.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials.
- I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I agree that the school is not liable for any damages arising from use of the Internet facilities.
- I understand that my son's/daughter's activity will be monitored and that the school will contact me if they have concerns about any possible breaches of the Internet Safety Rules or Pupil Acceptable Use Agreement.
- I understand not to upload any photos of St Thomas of Canterbury pupils at any school event (for example, assemblies/sports days/plays or school trips) onto a social media site.
- I understand that everything posted on a social networking site should be deemed as open to the public and it is therefore unacceptable to use this as a forum for posting inappropriate, damaging or malicious comments about the school or any members of the school community. (I will approach the class teacher and/or Head teacher with any concerns or issues I have with my child's education)

Many Thanks

Mr Jo Robinson

(E-Safety Coordinator and CEOP Ambassador)

Parent / Carer and Pupil Acceptable Use Agreement Form

Please sign and return this form to school

Parent/Carer Name:	Parent Signature:
	Date:

Pupil Acceptable Use Agreement

Your child needs to sign in the boxes below to show that they have read, understood and agree to the Pupil Acceptable Use Agreement relevant to their Key Stage. This will also be covered in class.

I understand the Pupil Acceptable Use Agreement for using technology, internet, email and online tools safely.

Pupil Name:	Class:
Pupil Signature:	Date:

Staff and Governors AUP

Staff Acceptable Use Policy Agreement

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

- **Systems -** I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, email and social media sites**.**

- **Misuse** - I will ensure that school owned information systems use will always be compatible with my professional role. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

- **Private Use** - I understand that school information systems may not be used for private purposes, without specific permission from the head teacher.

- **Logging in/out** - To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

- **Passwords** - I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word) and update regularly.

- **Software** - I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission.

- **Copyright** - I will respect copyright and intellectual property rights.

- **Data Protection** - I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1988. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.

- **Personal Information** - I will not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are secured and encrypted. Where possible I will use the School Learning Platforms to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.

- **Reporting** - I will report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator and/or the e-Safety Coordinators as soon as

possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Team. I know the CEOP Report Button.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the Head Teacher and ICT Technicians.

- **Communication** - I will ensure that any electronic communications with pupils and parents are compatible with my professional role.

- **My Professional Role** - My use of ICT and information systems will always be compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. If my mobile phone has a camera, I will not use it to take images of children in my care, I will always use a school based device. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

- **Publishing of Material** - I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.

- **Teaching E-Safety** - I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

- **Social Networking Sites** – 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 have read and understood the school's Social Media Policy.

- **Reporting -** I will report any incidents of concern regarding children's or staff safety to the school e-Safety Coordinator, Child Protection Teacher or Head Teacher.

- **Monitoring** - I understand that the school may monitor my information systems and Internet use to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read, understood and agree with the Staff Acceptable Use Policy

Signed: ……..……(Printed) ……

Date: …… School: ……

Record of Staff Training

Staff Name	E-Safety Training Attended	Code of Conduct Signed	Date

Pupil Acceptable Use Agreement Form – Class Teacher

I have read, understood and agree to the rules in the Pupil Acceptable Use Agreement.

	Pupil Name	Class	Signature	Date
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				
34				

Appendix H
Online Incident Log Sheet

Pupil Name: ……

Date of Incident:		**Class:**	
Description of incident:			
Action taken:			
Member of staff reporting/dealing with incident:			

Signed …….. Date ……..

Pupil Name: ……

Date of incident		**Class**	
Description of incident:			
Action taken:			
Member of staff reporting/dealing with incident:			

Signed …….. Date ……..

Appendix I – Photographs, Videos and Other Images

Use of Photographs, videos and other images within School

This applies to all staff, volunteers and students on work placement.

There are a number of things that you need to address when using images of people, especially children, some of which is contained in the Data Protection Act 1998:

- You must get the consent of all parents of children appearing in the photograph or video/DVD image before it is created
- You must be clear why and what you'll be using the image for and who will see it
- If you use images from another agency, you need to check that the agency has obtained informed consent

Safeguarding issues:

- Use equipment provided by the school to take the images and not personal devices
- Download and store images in a password protected area of the school network not on personal computers
- When images are stored on the system they should be erased immediately from their initial storage location e.g. camera
- Don't use full names or personal contact details of the subject of any image you use
- Children and families fleeing domestic abuse may be recognised via photos/images and whereabouts revealed to an abusive partner
- No images of a looked after child should be created or used without prior consent from Children's Social Care
- Don't use images of children in swimming costumes or other revealing dress – this reduces the risk of inappropriate use
- Always destroy images once consent has expired or the child has left your school

Consider:

- Are CCTV (security) cameras sited where they may compromise the privacy of individuals?
- How public are your display boards?
- What is the purpose and audience of video's and DVD's you have created?
- Are all of your images and media securely stored at your school?
- Images on websites, and other publicity can become public and outside your control
- Any implications of using images offsite
- The press are exempt from the Data Protection Act, if you invite them to your premises or event, you need to obtain prior consent from parents of children involved
- Including images from different ethnic groups and those of disabled children
- Check out any copyright implications

The Information Commissioner's Office guidance advises that photographs taken for personal use e.g. by parents at special events, at an education setting are not covered by the Data Protection Act.

Useful links/resources:

- **Photographs and Videos, Information Commissioners Office, at:** http://www.ico.gov.uk/for_the_public/topic_specific_guides/schools/photos.aspx

Appendix J

St Thomas of Canterbury School
Photographs and Videos of Children

The value of taking photographs and videos of children's learning, recording memories of special events and celebrating achievements significantly outweigh any potential safeguarding risks.

We use photographs and video footage for a wide range of purposes, including:

- It is our policy to use photographic and video evidence as part of our assessment evidence.
- We celebrate children's learning by posting images on our class blogs and on Twitter.
- In Reception, the team are using an app to record steps in children's learning through photographs and these are emailed to parents in real-time.
- Our school newspaper uses photographs to support its stories.
- Key events are photographed as a memory and this is often shared with other parents or in our publications.
- Parents take photographs at school events for their memories.
- The children take photographs as part of their media curriculum.
- A photography company takes class photographs which are shared with other parents.
- We often film children's performances.
- We use images in our prospectus and other marketing materials.
- Occasionally, journalists visit the school to cover a positive story and take photographs of our children to go into their newspaper.
- We use photographs and videos for many other educational reasons.

How do we ensure that images and video footage is used safely?

- We use equipment provided by the school to take the images and staff do not use personal devices.
- We download and store images in a password protected area of school network not on personal computers.
- When images are stored on the network they are erased immediately from their initial storage location.
- We do not use names or personal contact details of the subject of any image we use. First names are posted online without an image but never with an image so that children are not identifiable.
- We do not use images of children in swimming costumes or other revealing dress – this reduces the risk of inappropriate use.

Safeguarding our children is the number one priority and the school takes responsibility for using the images safely.

It is assumed that all parents give their consent to the school using photographs and videos as outlined above.

Protecting Identity

There may be genuine reasons why a parent or carer would need to protect a child's identity, such as:

- Children and families fleeing domestic abuse may be recognised via photos/images and whereabouts revealed to an abusive partner.
- A child may be in public care and their identity or location needs to be protected.

Even in the above cases, our policy protects the children's identity as we would never put a full name on the website or any name with an image therefore internet search engines could not trace an image of a particular child. If you have a specific safeguarding reason such as this and you do not wish for the school to use your child's image in this way, please make a confidential appointment to see Miss O'Neill or Mrs Wileman, our Safeguarding Team, who can discuss this with you further and ensure that we put in place the necessary precautions.

Appendix K - Resources and Organisation

RESOURCES

ThinkUKnow - http://www.thinkuknow.co.uk/

Childnet International - http://www.childnet-int.org/

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

Chatdanger - http://www.chatdanger.com/

Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx

NCH - http://www.stoptextbully.com/

ADVICE FOR PROTECTING CHILDREN

Child Exploitation and Online Protection Centre (CEOP) - http://www.ceop.gov.uk/

The Byron Review ("Safer Children in a Digital World") http://www.dcsf.gov.uk/byronreview/

CYBER BULLYING

http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

http://www.teachers.gov.uk/wholeschool/behaviour/tacklingbullying/safetolearn/

Cyberbullying.org - http://www.cyberbullying.org/

SOCIAL NETWORKING

Digizen – "Social Networking Services" - http://www.digizen.org.uk/socialnetworking/

DATA PROTECTION

Information Commissioners Office - Data Protection:
http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx