Park Street Church of England (VA) Primary School
Lower Park Street, Cambridge CB5 8AR
Tel: 01223 576922
Email: office@parkstreet.cambs.sch.uk
www.parkstreet.cambs.sch.uk

Online Safety Policy & Acceptable Use of ICT

Author: Sarah Hawker (Headteacher; 24/02/2023)
Approved by: Nigel Moorhouse (Chair of Governors; 05/03/2023)
Version: 1.0
Date: 24/02/2023

Our online and offline behaviour principles are rooted in Christian values, such as love, compassion, forgiveness and reconciliation.

The fruit of the Spirit is love, joy, peace, forbearance, kindness, goodness, faithfulness, gentleness and self-control. Against such things there is no law. **Galatians 5:22-23**

"School should be, for the less fortunate, what home is for the more fortunate. A place where there is work but also laughter, a place where there is law but also grace, a place where there is justice but where there is also love." **Sir Alec Clegg – 1974**

It is the view of our school that we aspire to the principles laid out above. Our steadfast intent is, in line with our Christian ethos, to provide an environment in which every member of our community is treated with respect and trust.

1. Terms of Reference

1.1. This policy shows our school's ability to:

- protect and educate pupils and staff in their use of technology
- have the appropriate mechanisms to intervene and support any incident where appropriate.

Inspecting online safety in Schools, Ofsted 2012

1.2. This policy takes into account guidance from:

- Keeping Children Safe in Education, September 2022
- Teaching Online Safety in Schools guidance – DfE, June 2019
- Education for a Connected World – UKCIS, June 2020
- National Curriculum in England - Computing - DFE, Sept 2014
- Relationships and Health Education – DfE, July 2020

2. Background

2.1. The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practice embedded in our school and followed by the whole school community.
- The infrastructure and how it is set up to keep pupils safe online, including filtering, monitoring, and preventing and responding to online safety incidents.
- A progressive, relevant age-appropriate online safety curriculum for all pupils which (as a minimum) meets the requirements of the National Curriculum for Computing and the statutory Relationships and Health Education

2.2. Online safety in schools is primarily a safeguarding concern and not a technology one. Therefore, this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to: Safeguarding and Child Protection Policy

- Personal Social and Health Education (PSHE) policy and curriculum
- RSE policy and scheme of work
- Safer Working Practices
- Data Protection Policy
- Behaviour Policy

- Anti-Bullying Policy
- School Complaints Procedure
- Our 'Teach Computing' curriculum and progression
- Whistleblowing Policy

2.3. This policy must be read alongside the Acceptable Use of ICT for Staff (Appendix B), and for Pupils (Appendices C and D). These outline the expectations and sanctions which apply to staff and pupil use of technology.

The development of our online safety policy involved:

- The Headteacher and Designated Safeguarding Lead
- The Deputy Designated Safeguarding Lead
- The Computing Subject Leader
- The governor responsible for Safeguarding

2.4. This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It is shared with all staff via 'My Concern' and a staff meeting and is readily available on the school network and website, where it is also available to parents.

2.5. All staff must be familiar with this policy and Acceptable Use of ICT (Appendix B). Online safety is an important part of our school's approach to safeguarding, and all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

3. Rationale

3.1. At Park Street CofE Primary School, we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the misuse of technology can put young people at risk within and outside the school.

The risks they may face can broadly be categorised into the '3 C's' **Contact, Content** and **Conduct** (Livingston and Haddon) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing of Self-Generated Indecent Images
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

3.2. While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school, and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops / iPads / Chromebooks / desktops - staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
- Some staff (mostly teachers) have access to school systems beyond the school building (e.g. Arbor, Microsoft 365 and Google Workspace).
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards
- Staff level internet access
- Subscription services for education such as TT Rock Stars, Twinkl, Mathletics, White Rose Maths, Letter Join, IDL, Master the Curriculum (for EYFS and SEN) Provision Map, Spelling Frame, Letterjoin, Supersonic Phonic Friends, Phonics Play, Early Years Staffroom iMoves, My Concern Typing Club, Arbor, etc

Pupils:

- Curriculum laptops / iPads / Chromebooks / desktops including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources
- Cloud platforms / online tools providing pupils with access within and beyond the school gates

3.3. Where the school changes the use of existing technology or introduces new technologies which may pose risks to pupils' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

4. The online safety curriculum

4.1. When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age-appropriate online safety curriculum is clearly documented in the National Curriculum for Computing (England) and the statutory Relationship and Health Education.

4.2. At Park Street C of E Primary School we believe that a comprehensive program of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool, so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

4.3. Our online safety curriculum is covered using the Cambridgeshire PSHE Service Primary Personal Development Programme, and our 'Teach Computing' scheme, with reference to UKCIS's Education for a Connected World

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials and is linked to demonstrating safe practice in our online learning platform
- Key online safety messages are delivered and reinforced through cross-curricular opportunities such as emailing, researching, blogging and communicating in appropriate online environments.
- Focus events to raise the profile of online safety for our pupils and school community

5. Continued Professional Development

5.1. Staff at Park Street C of E Primary School receive up-to-date information and training on online safety in the form of staff meetings and updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.

5.2. Nominated members of staff receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.

5.3. New staff receive information on the school's Acceptable Use of ICT (Appendix B) as part of their induction, including advice on Protecting their Professional Reputation Online.

5.4. All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

6. Mobile phones and use of 3G and 4G data in school

6.1. Children are not allowed to use mobile phones for any reason on the school premises. If they bring one for safety in travelling to and from school, it must be handed in to the office on arrival, and collected at the end of the day. Staff must keep their phones out of sight when in the building; although personal devices can be brought to Jesus Green when they might be used to call for help.

6.2. Similarly, children are asked to hand in 'smart watches', if these are able to access the internet.

6.3. Parents are asked, in most cases, to refrain from taking photographs, video or recordings of children during performances or church services. If photography is allowed (which would only be in the case where we are confident that all children have given permission) they are instructed to refrain from uploading to social media.

7. Monitoring, and averting online safety incidents.

7.1. The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following Safeguarding procedures where appropriate.

7.2. The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained The ICT Service on behalf of the local authority. Safeguards built into the school's infrastructure include:

- Secure, private EastNet internet connection to each school with a direct link to the National Education Network.
- Managed firewalling running Unified threat management (UTM) that provides restrictions on download of software, apps and file types from known compromised sites.
- Foundation DDoS mitigation service, security analysts carefully monitor the patterns of traffic across the network.

- Enhanced web filtering provided to all EastNet sites as standard.
- Optional SSL decryption available on web traffic to allow for greater visibility of sites being accessed and requested.
- Antivirus package provided as part of EastNet Connection.

7.3. Staff also monitor pupils' use of technology and, specifically, their activity online. This is achieved through a combination of:

- Appropriate levels of supervision when pupils are using online technologies
- Robust firewall which prevents children accessing inappropriate materials
- Staff check pupils browsing history regularly, especially if they have any suspicions
- Staff use of the schools' internet can also be monitored and investigated where needed.

7.4. A system of staff and pupil passwords is in place to enable appropriate access to the school network. All members of staff have individual, password protected logins to the school network / cloud service / MIS systems.

- Visitors to the school can access part of the school systems using a generic visitor login and password.
- The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.
- School staff and pupils are not permitted to connect personal devices to the school's wireless network and a guest wireless key is issued to visitors on a case-by-case basis.

7.5. Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks to an acceptable level.

8. Responding to online safety incidents

8.1. It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
- If an online safety incident occurs, Park Street CofE Primary School will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts, restricted access to systems as per the school's Acceptable Use of ICT (Appendix B), or reporting incidents to the police and other authorities).

8.2. In addition, the Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.

8.3. With this in mind, the Headteacher may decide to apply sanctions and / or procedures to incidents which occur outside of schools if they deem it appropriate.

8.4. The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

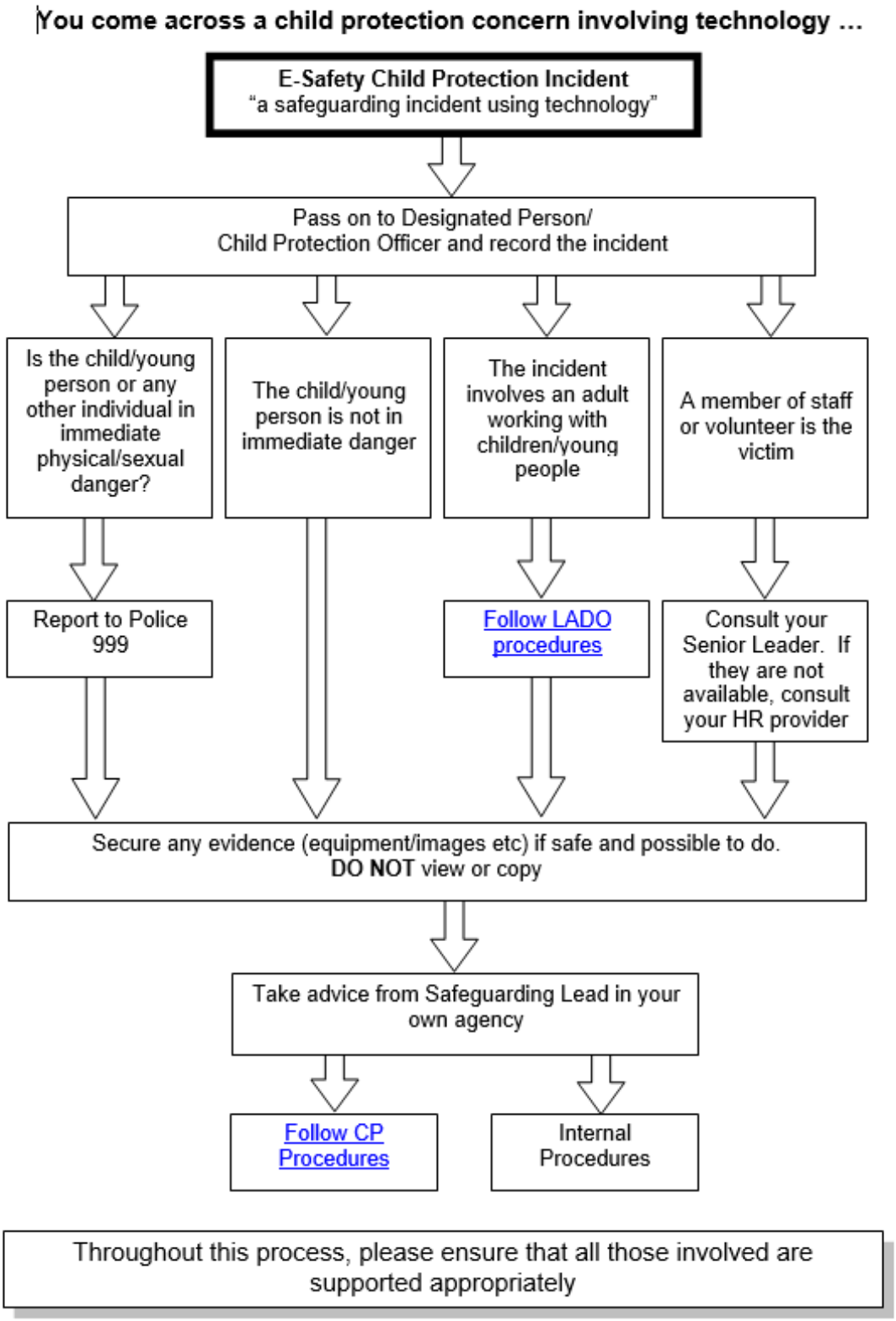
NB: In our school, the likelihood of these types of instances occurring are already reduced as we don't allow pupils to use personal devices in school.

8.5. Where the school suspects that an incident may constitute a Safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated in Appendix A.

9. The school's response to harmful sexual behaviour

9.1. We work to prevent sexual harassment, online sexual abuse and sexual violence through our whole school approach. This begins with our rules and values: 'Respect' is consistently highlighted in all behaviour management situations as one of our three rules and one of our six values. Children learn to respect each other through Collective Worship, Religious Education as well as through our PSHE and RSE curricula, which include the addressing of issues of consent. In addition, we use the NSPCC 'Pants' materials (https://learning.nspcc.org.uk/research-resources/schools/pants-teaching) regularly in circle time and PSHE lessons. All staff, including the lunchtime supervisors, are aware that sexual harassment is likely to happen in and around the school and are vigilant for signs that this has occurred. When an incident is reported, it is addressed in a timely way, using a zero-tolerance approach, with an appropriate consequence that gives children the opportunity to make amends and be supported to move forward. Parents are also informed, and are asked to reinforce this firm approach with the children at home. We refer to the 'Safer Spaces Toolkit', the 'Child Sexual Behaviour Assessment Tool' and the 'Primary Harmful Sexual Behaviours Risk Assessment' (all developed by Cambridgeshire Safeguarding and the PSHE Service), and all relevant incidents are reported using the 'Prejudice Reporting in Education' system.

Appendix A: Process for responding to online safety incidents.



Appendix B: Acceptable Use of ICT for Staff

Our statement on Acceptable use of ICT is intended to protect the school, pupils and staff in terms of safeguarding, wellbeing and information security.

When using the school's ICT equipment and other information systems, or personal ICT equipment where referenced, all staff will comply with the following statements. Failure to comply could result in disciplinary action.

Use of school-based equipment

- They will access the internet and other ICT systems using an individual username and password, which they will keep secure. They will ensure that they log out after each session and never allow other users to access the internet through their username and password. They will report any suspicion, or evidence that there has been a breach of personal security, in relation to access to the internet or ICT systems, to the Headteacher.
- All passwords they create will be in accordance with the school Online Safety Policy. They will ensure that they use a suitably complex password for access to the internet and ICT systems.
- They will not share passwords.
- They will seek consent from the Headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- They will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If they encounter any such material, they will report it immediately to the Headteacher.
- They will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in their care.
- They will not attempt to bypass any filtering and/or security systems put in place by the school. If they suspect a computer or system has been damaged or affected by a virus or other malware, they will report this to the Headteacher.
- They understand their personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- They will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
- They will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.
- Any information asset, which they create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection controls. (For example spreadsheets/other documents created from information located within the school information management system).
- They will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from an IT technician.

- They understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- They understand that their files, communications and internet activity may be monitored and checked at all times to protect their own and others' safety, and action may be taken if deemed necessary to safeguard me or others.

Social Networking

- They must not use social media tools to communicate with current or former pupils under the age of 18.
- They will not use any social media tools to communicate with parents unless approved by the Headteacher.
- They will set and maintain their profile on social networking sites to maximum privacy and give access to known friends only.
- Staff must not access social networking sites for personal use during school hours.
- If they experience any derogatory or slanderous comments relating to the school, colleagues or their professional status, they will take screenshots for evidence and escalate to the Headteacher.

Managing digital content

- They will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- They will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved.
- Under no circumstances will they use any personally-owned equipment for video, sound or images without prior consent from a member of the Senior Leadership Team.
- When searching for images, video or sound clips, they will ensure that they or any pupils in their care are not in breach of any copyright licencing.
- They will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- They will ensure that any images taken on school-owned devices will be transferred to the school network (storage area/server) and deleted as soon as possible from the memory card.
- They will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this They will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Email

- They will use their school email address for all correspondence with staff, parents or other agencies and they understand that any use of the school email system will be monitored and checked. They will under no circumstances use their private email account for any school-related business.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.

- They will ensure that any posts made on websites or via electronic communication, by either themselves or the pupils in their care, will not damage the reputation of the school.
- They will seek permission if they need to synchronise any school email account with a personally-owned handheld device.
- They will take care in opening any attachments sent by email. They will only open emails and associated attachments from trusted senders.
- Emails sent to external organisations will be written carefully and, if necessary, authorised before sending to protect themselves. As and when they feel it necessary, they will carbon copy (cc) the Headteacher, line manager or another suitable member of staff into the email.
- They will ensure that they manage their email account, delete unwanted emails and file those they need to keep in subject folders.
- They will access their school email account on a regular basis to ensure that they respond in a timely manner to communications that require their attention.

Mobile phones, smart watches and devices

- They will ensure that their mobile phone and any other personally-owned device is switched off or switched to 'silent' mode during school hours.
- Bluetooth communication should be 'hidden' or switched off. Mobile phones or smart watches or other devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances. Staff may take their personal phones to Jesus Green but these are only for use in an emergency. They are to be kept hidden at all other times.
- They will not contact any pupils on their personally-owned device.
- They will not use any personally-owned mobile device to take images, video or sound recordings of children at school.

Learning and teaching

- In line with every child's legal entitlement, they will ensure they teach an age-appropriate online safety curriculum.
- They will support and promote the school Online Safety Policy at all times. They will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- They will ensure that they are aware of their individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community. They will report any concerns or incidents, following the school's safeguarding procedures, and will take seriously any incidents of harmful sexual behaviour reported or witnessed, online or in person.
- They understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of their own resources at all times.

Appendix C: Acceptable Use of ICT for KS1 Pupils

Our statement on Acceptable use of ICT is intended to protect the school, pupils and staff in terms of safeguarding, wellbeing and information security.

When using the school's ICT equipment and other information systems, or personal ICT equipment where referenced, all KS1 pupils will comply with the following statements. Failure to comply could result in sanctions.

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell a trusted adult if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show a trusted adult if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email when at school
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

I am aware that:

- anything I do on the computer may be seen by someone else
- there is a CEOP report button and know when to use it

Appendix D: Acceptable Use of ICT for KS2 Pupils

Our statement on Acceptable use of ICT is intended to protect the school, pupils and staff in terms of safeguarding, wellbeing and information security.

When using the school's ICT equipment and other information systems, or personal ICT equipment where referenced, all KS2 pupils will comply with the following statements. Failure to comply could result in sanctions.

These rules will keep us safe and help us to be fair to others.

- I will keep my passwords for logging in to any computer or application to myself – if I think others know my passwords I shall tell my teacher.
- I shall use the online activities and sites which school allows me to access from home appropriately.
- I will not bring in memory sticks into school unless I have been given permission.
- I will not bring my own mobile device/ phone into school unless I am given permission from my teacher. If I do need to bring it in, I may not use it without permission from my teacher.
- If the computer asks for any update, I shall check this with my teacher.
- I will only use the computer for things my teacher has told me to.
- I will not use the internet to access unsuitable material.
- The messages I send will be polite and respectful.
- I will always report anything that I feel is unkind or makes me feel unsafe or uncomfortable to my teacher. I will not reply to any nasty messages.
- In school, I will only use my school e-mail and only e-mail people my teacher has approved.
- I will always keep my personal details private (e.g. my name, mobile phone number, family
- information, journey to school, pets, hobbies).
- I will not register my details with online activities and websites without the permission of my teacher.
- I will not share files or photos without the permission of my teacher.
- I will not copy text or pictures from the internet and pretend it is my own work.
- I will never meet an online friend without taking a responsible adult who I know with me.
- I understand that the school will check my computer files and will monitor the internet sites I visit.
- I will treat computer equipment, like all school equipment, with care and respect.
- I know that if I break the rules I might not be allowed to use a computer.

I am aware that:

- there is a CEOP report button and know when to use it
- anything I share online may be monitored
- one I share anything online, it is completely out of my control and may be used by others in a way that I did not intend.