Policy Name	E-Safety Policy
Frequency of Review	2 years
Reviewed on:	June 2017
Reviewed by:	Learning Committee
Next review (date)	June 2019

E-Safety Policy

This policy was written in January 2010 as the ICT Acceptable Use Policy and reviewed in March 2017. The policy has been renamed as the E-Safety Policy, which includes the Acceptable Use Policies for staff and students. It was researched and produced by the Computing Subject Lead, Designated Person for Child Protection, Head Teacher and Governors. The designated members responsible for Internet safety in the school are the Designated Person for Child Protection and the Computing Subject Lead.

1. Aims

The aims of this E-Safety Policy are to:

- Ensure safeguarding measures are in place for adults and children in school in relation to e-safety.
- Ensure the policies and practices embedded in the school are adhered to by the whole school community.
- Provide an infrastructure to monitor, prevent and respond to e-safety incidents.
- Provide a progressive, age appropriate e-safety curriculum for all pupils.
- Ensure that pupils benefit from all learning opportunities offered by the internet resources provided by the school and resources provided by the county (e.g. Starz learning platform) in a safe and controlled manner.
- Ensure that all staff benefit from internet access, with clear guidance on safe and acceptable use.
- Provide guidance to staff and pupils about the acceptable use of mobile technologies, both the school's and personal items that are brought into school.

E-Safety in school is primarily a safeguarding issue and not computing/technology one. Therefore this policy should be read in conjunction with the school's other safeguarding policies including, but not limited to:

- Keeping Children Safe in Education
- Safeguarding and Child Protection Policy
- Code of Conduct Policy
- Behaviour Policy and Principles
- Communication Code
- Personal Social and Health Education Policy
- Persistent Complaints and Harassment Policy

- Tackling Bullying Policy
- School Complaints Procedure
- Whistleblowing Procedure
- Cambridgeshire Progression in Computing Capability Materials
- school's guidance on use of mobile phones included in the staff handbook
- Cambridgeshire County Council's Guidance for schools and other establishments on the use of images.

This policy must be read alongside the staff and pupil Acceptable Use Policies (AUPs) attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology. All staff must sign the relevant AUP to access the school's system.

As E-Safety is an important part of strategic leadership within the school, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Person for Child Protection and Governors.

2. Rationale

At Morley Memorial 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 use of these new technologies 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.
- 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 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.

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. E-Safety issues can also affect adults who work or are associated with the school.

Technologies regularly used by pupils and staff include:

a. Pupils

- School laptops including filtered access to the internet and pupil level access to areas of the school network.
- iPads for Special Education Needs.
- Cameras and peripherals including programming resources (Beebots etc.)

b. Staff

- Staff laptops and desktops in the office including staff level internet access, server access, and in some circumstances, access from home (e.g. Target Tracker and email).
- iPads for preparing and delivering pupil activities, for Special Education Needs.
- Class cameras and other peripherals such as visualisers and interactive whiteboards.

3. Use of ICT in Morley

The purpose of Internet access in this school is to:

- raise educational standards,
- support the professional work of staff and
- enhance the school's management, information and business administration systems.

Teachers and pupils will have access to web sites worldwide (including museums and art galleries) offering educational resources, news and current events.

Access to the Internet is a planned part of the curriculum that enriches and extends learning activities and is integrated into the class schemes of work. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for Internet use.

Different ways of accessing information from the Internet are used depending upon the nature of the material being accessed and the age of the pupils, for example:

- by teacher (or sometimes other-adult) demonstration;
- by teacher-prepared materials, rather than the open internet;
- pupils may be given a suitable web page or a single web site to access;
- pupils may be provided with lists of relevant and suitable web sites which they may access;
- pupils are expected to observe the Rules of Responsible Internet Use and are informed that checks can and will be made on files held on the system and the sites they access.
- pupils will be educated in taking responsibility for their own Internet access.

The use of other personal technology is allowed in school as part of a pre-arranged educational activity, with permission from a member of the Senior Leadership Team (SLT) or Computing Subject Leader. Inappropriate use is in direct breach of the school's E-safety Policy and Acceptable Use Policy, outlined below and in the appendices.

4. Expectations Of Use

a. Pupils

Children and their parents will be expected to sign an Acceptable Use Policy detailing expectations of behaviour and the consequences of violating this agreement (see appendices).

- At Morley Memorial, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in school. This includes materials they choose to access, and language they use.
- Pupils using the World Wide Web are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to the supervising adults so that the appropriate action may be taken.
- Pupils are expected not to use any abusive language in their email communications and contact only people they know or those the teacher has approved. They have been taught the rules of etiquette in email and are expected to follow them. They will not send abusive or unwanted communications to other pupils.
- All pupils and their parents/guardians are expected to have read and agree the Acceptable Use Policy and be aware of their rights and responsibilities.

The consequences of breaking these rules will depend on the nature of the violation but could include some or all of the following sanctions:

- The withdrawal of internet use
- The suspension of Starz accounts
- Bringing in external agencies such as the police or social services. (This will be done with reference to our Child Protection Policy.)

Misuse by pupils of other technologies (e.g. mobile phones) will result in a complete ban and/or confiscation of these devices. (See the school's Use of Mobile Phones Policy for further information.)

b. Staff

- Staff are responsible for their own behavior on the Internet; this includes materials they
- choose to access, and language they use.
- Staff using the internet are expected not to deliberately seek out offensive words or images; or to store or view offensive words or images on their computer; or to access inappropriate sites of any other nature (e.g. gambling, betting, online gaming).
- Staff are expected to use appropriate language in their email communications.
- The use of the internet or other forms of mobile communication for personal use during teaching hours is allowable but should be moderated to reasonable level which does not affect the teaching and learning of the pupils, preferably during breaks from the classroom; this level will be at the discretion of the head teacher.
- All members of staff using social networking sites or other forms of public communication should be aware of the visibility of their communications and the implications of bringing the school's reputation into disrepute.

The consequences of breaking these rules will depend on the nature of the violation and will be dealt with in line with the schools Disciplinary procedure. This may involve suspension or the involvement of external agencies such as the police or social services if deemed serious enough. This is covered in section 6 of the disciplinary procedures, "Gross Misconduct".

5. <u>E-safety Curriculum</u>

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

e-safety curriculum is clearly documented in the National Curriculum for Computing which states that:

- **At KS1:** use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- **At KS2:** use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

At Morley Memorial Primary School we believe that a comprehensive programme of e-safety education is vital for developing our pupils' ability to use technologies safely. We believe that children will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

This is achieved using a combination of:

- Activities drawn from a selection of appropriate materials including the Cambridgeshire Progression in Computing Capability Materials and ACE (Accredited Competence in E-Safety) Scheme of Work developed by Cambridgeshire ICT Services.
- Using the Starz+ online learning platform.
- Key e-safety messages delivered and reinforced through cross curricular opportunities throughout the year (including during designated computing lessons) and through E-Safety Day activities.

Key e-safety messages include, but are not limited to:

- personal e-safety (not giving personal details out online)
- Cyber bullying and how to deal with it
- The importance of keeping usernames and passwords confidential
- Dealing with unwanted images or material, including pop-ups
- Good etiquette in ICT use (e.g. user names to reflect sender)
- "Whistle blowing"

In common with all other media (such as magazines, books and video), some material available on the Internet is unsuitable for pupils. The school will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet. Morley Memorial Primary School use a Cambridgeshire County Council "filtered" Internet Service, which will minimise the chances of pupils encountering undesirable material.

Children at Morley Memorial Primary School will normally only be allowed to use the Internet when there is a responsible adult present to supervise. However, it is unrealistic to suppose that the teacher's attention will always be directed toward the computer screen. Members of staff will be aware of the potential for misuse, and will be responsible for explaining to pupils the expectation we have of pupils.

Teachers will have access to pupils' emails as part of their Starz+ accounts and will check other Internet related files on a regular basis to ensure expectations of behaviour are being met.

6. Continued Professional Development

Staff receive information and training on e-safety issues in the form of staff meetings and updates from the Computing Subject Leader, as well as training from external providers where

appropriate. New staff receive information on the school's AUP as part of their induction. All staff are made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to in the event of misuse of technology by any member of the school community.

7. School Website

The main purpose of our school website is to provide information. Our school website will not only tell the world that our school exists, but it will provide information for our pupils and parents, promote the school to prospective ones and publish the statutory information required by the Department for Education.

The school website will adhere to these e-safety principals in the following ways:

- The website will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff.
- The publication of children's work will be decided by a teacher.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Photographs and video focusing on individual children will not be published on the school website without parental permission.
- Permission for the use of images will be gathered from parents on entry to the school and kept centrally in the office.
- The school website will avoid publishing the full names of individuals in a photograph.
- The school will ensure that the image files are appropriately named and will not use pupils' names in image file names if published on the web.

8. Monitoring and Averting E-Safety Incidents:

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

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service. Safeguards built into the school's infrastructure include:

- Secure, private Cambridgeshire Public Service Network (CPSN) provided internet connection to each school with a direct link to the National Education Network. Managed firewalling.
- Base line and enhanced filtering provided by the Local Authority approved filtering system.
- CPSN provided Sophos antivirus package.
- Council funded email system for all school staff with direct internal routes to the council for trusted email communications.
- Restrictions on download of software, apps and file types from known compromised sites.

Staff also monitor pupils' use of technology and, specifically, the internet.

- Pupils' use of online services (including the World Wide Web) are supervised in school at all times.

- Staff are also able to monitor pupils' activity in the Starz+ learning platform, allowing them to identify inappropriate or concerning online behaviour, as well as respond to reports of any such behaviour from pupils or parents.

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.
- Visitors to the school can access part of the network using a generic visitor login and password.
- The school's network is accessed using a wireless connection. A the time of installation the wireless network was encrypted to a suitable standard as 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.

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 as much as possible.

9. Responding to E-Safety Incidents

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

- Staff responses to e-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 e-safety incident occurs, Morley Memorial Primary School will follow its agreed procedures for responding, including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix).

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 e-safety incidents which may take place outside of the school but has an impact within the school community.

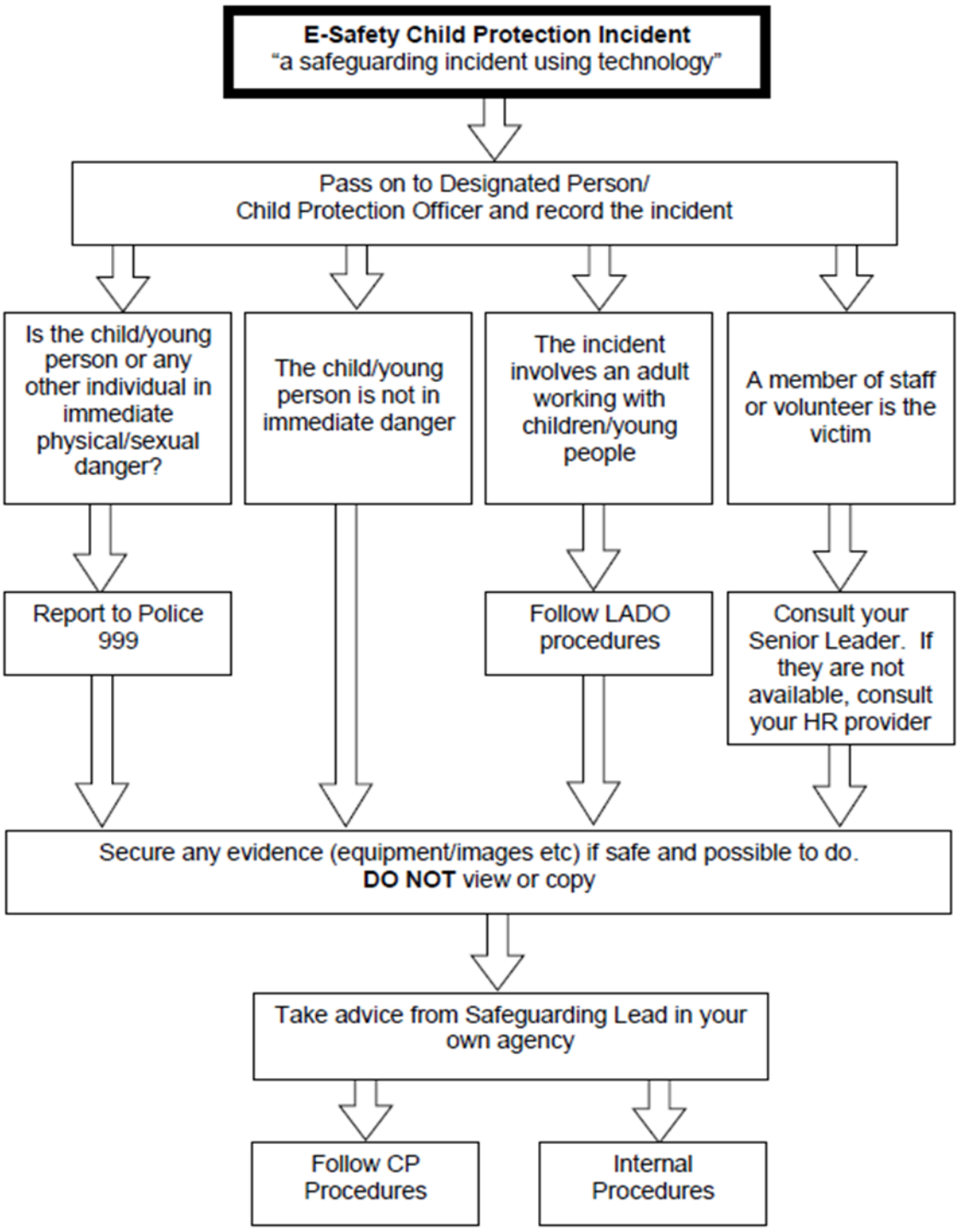
- With this in mind, the Headteacher may decide to apply the sanctions and/or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

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 with parents (where appropriate) before taking any further action.

Where the school suspects that an incident may constitute a Child Protection issue, the usual Child Protection procedures will be followed. This process is illustrated in the diagram below.

You come across a child protection concern involving technology …



Pupil Acceptable Use Policy (KS1), Morley Memorial Primary School

This is to be read through with your parent(s) and then signed. You will be allowed Internet Access after this is returned to school.

- I will use the school's ICT equipment and tools (including computers, cameras, Starz etc.) for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.
- I will only use the internet and email when an adult is nearby.
- I will not share my passwords with other people and will tell my teacher if I think someone else knows them.
- I will ask an adult before opening an email from someone I don't know.
- I will only email or contact someone I know or those the teacher has approved.
- I will not share details about myself such as surname, phone number or home address.
- I will ask if I need to look at other peoples' work on the computer.
- I will try my hardest to only send messages which don't upset other people.
- I will ask my teacher before using photos or video.
- I will not downloaded files or programmes to the computer from the Internet.
- If I see something on a screen which upsets me, I will always tell an adult.

I will do my best to follow these rules because I know they are there to keep me and my friends safe. If I don't follow these rules, I know that my teacher may stop me using technology at school and talk to my parents about how I use technology.

I have read through this agreement with my child and agree to these safety restrictions.

Signed: _____ (Parent/Responsible Adult)

Name of child: _____

Pupil Acceptable Use Policy (KS2), Morley Memorial Primary School

This is to be read through with your parent(s) and then signed. You will be allowed Internet Access after this is returned to school.

- I will use the school's ICT equipment and tools for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.
- I will only use the Internet if a teacher or teaching assistant is in the room with me.
- I will only delete my own files unless my teacher gives me permission to delete someone else's. I will not look at other people's files without their permission.
- I will keep my passwords private and tell an adult if I think someone else knows them. I know that my teacher can change my Starz password if needed.
- I will only open e-mail attachments from people who I know or an adult has approved. If I am unsure about an attachment or e-mail, I will ask an adult for help.
- I will only email or contact people I know or those the teacher has approved.
- I will not give my own personal details such as surname, phone number or home address or any other personal details that could be used to identify me, my friends or my family. If I have to use an online name I will make one up!
- I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.
- I will not downloaded files or programmes to the computer from the Internet.
- I will not bring in work on discs, CDROMs or memory sticks from home; homework can be emailed or uploaded onto Starz instead.
- I will never arrange to meet someone I have only ever previously met online. It could be dangerous.
- I will not deliberately look for, save or send anything that could be unpleasant or upsetting. If I find anything via Internet, e-mail or mobile phone that is upsetting or makes me feel uncomfortable, I will tell a teacher or responsible adult.

I will do my best to follow these rules because I know they are there to keep me and my friends safe.

If I don't follow these rules, my teacher may:

- Speak to me about my behaviour.
- Speak to my parents about my use of technology.

- Remove me from online communities or groups.
- Turn off my access for a little while.
- Not allow me access to use laptops / computers to access the internet or particular programmes.
- Take other action to keep me (and others) safe.

I have read through this agreement with my child and agree to these safety restrictions.

Signed: _____ (Parent/Responsible Adult)

Name of child: _____

Staff Acceptable Use Policy, Morley Memorial Primary School

I have read through the E-Safety Policy and Acceptable Use Policy, and agree to the safety restrictions outlined in Section 4b of the E-Safety Policy and the restrictions outlines below:

Use of school based equipment

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements:

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the e-safety coordinator, office staff and ICT staff members (network managers).
- All passwords I create will be in accordance with the school e-safety Policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems.
- I will not share my passwords.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-safety coordinator/Head Teacher.
- I 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 my care.
- 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, I will report this to the ICT staff members (network managers).
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- I 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.
- I will only use school-owned or provided portable storage (USB sticks, SSD cards, portable hard drives etc).
- I 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 I 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 spread sheets/other documents created from information located within the school information management system).
- I 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 the ICT Staff Members (network manager).

- I 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.
- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.

Social Networking

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I will not use any social media tools to communicate with parents unless approved in writing by the Head Teacher.
- I will set and maintain my 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 I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the e-safety coordinator/Head Teacher.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I 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 as detailed in the E-Safety Policy (or any other relevant policy).
- Under no circumstances will I 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, I will ensure that I or any pupils in my care are not in breach of any copyright licencing.
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- I 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.
- I 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 I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Email

- I will use my school email address for all correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my 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.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will seek permission if I need to synchronise any school email account with a personally-owned handheld device.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.

Mobile phones and devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode during teaching periods.
- Bluetooth communication should be 'hidden' or switched off.
- Mobile phones or devices for personal use during school hours is allowable but should be moderated to a reasonable level which does not affect the teaching and learning of the pupils, preferably during breaks from the classroom; this level will be at the discretion of the Head Teacher.
- I will not contact any parents or pupils on my personally-owned device.
- I will not use any personally-owned mobile device to take images, video or sound recordings.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach an age appropriate e-safety curriculum.
- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.

I understand that failure to comply with these restrictions may result in disciplinary action being taken in line with the school's Disciplinary Policy.

Signed_____

Print_____

Counter signatory_____
(Computing Subject Leader or Head Teacher)