Online Safety Policy

Most Recent Review: September 2025

Date for Review: September 2027

CONTENTS

Introduction

Online Safety encompasses not only Internet technologies but also electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology. It provides safeguards and raises awareness to enable users to control their online experiences.

The Internet is an unmanaged, open communications channel. The World Wide Web, e-mail, blogs and social networking all transmit information using the Internet's communication infrastructure internationally at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by millions of people every day.

However, much of the material on the Internet is published for an adult audience and some is unsuitable for pupils. In addition, there is information on weapons, crime and racism access to which would be more restricted elsewhere. Pupils must also learn that publishing personal information could compromise their security and that of others.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- Content: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- Contact: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- Conduct: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- Commerce: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

For this reason, we need to protect our school by making it clear to pupils, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised" and ensure that all reasonable actions are taken and measures put in place to protect users.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2021'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

This policy operates in conjunction with the following school policies:

- Acceptable Use Agreement
- Data Protection Policy
- Safeguarding Policy
- Anti-Bullying Policy
- PHSE Policy
- RSE and Health Education Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedures
- Confidentiality Policy
- Remote Learning Policy

It has been agreed by the senior leadership team and approved by governors. The Online Safety Policy and its implementation will be reviewed every two years.

2. Roles and responsibilities

The governing board is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on a two year basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Head of School is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the Deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct annual light-touch reviews of this policy.
- Working with the DSL and Governing Body to update this policy on a 2-yearly basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school, with the support of the computing leader.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENDCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.

- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the Governing Body about online safety on a termly basis.
- Working with the Head of School, SBM and ICT technicians to conduct annual light-touch reviews of this policy.
- Working with the Head of School and Governing Body to update this policy on a 2 yearly basis.

ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Head of School.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and Head of School to conduct annual light-touch reviews of this policy.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Adhering to the Acceptable Use Agreement and other relevant policies.

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. Teaching and Learning

Why Internet Use is Important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. They will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

4. Potential threats

Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

Peer-on-peer sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.
The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.
The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy. Or in the instance of a staff member, the investigation will be undertaken by the Head of School in line with the Disciplinary Policy.

Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.
Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda.
Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.
Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Procedures. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.
Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Procedures.

Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation. Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Online hoaxes and harmful online challenges

For the purposes of this policy, an "online hoax" is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.
For the purposes of this policy, "harmful online challenges" refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.
Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.
The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country.

Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.
Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Head of School will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.
The DSL and Head of School will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- Cyber-enabled – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- Cyber-dependent – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.
The DSL and Head of School will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

5. Managing Online Safety

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be updated regularly.
- Security strategies will be discussed with the Enhance Academy Trust and Global Computing Solutions.

E-mail – NB – Our children are Under 8 so not usually accessing emails but…

Pupils

- must immediately tell a teacher if they receive offensive e-mail.
- must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- The forwarding of chain letters is not permitted.

Staff

All work-related emails should be written using a school email address. School email should be regarded as an official communication. Emails should be written in the same professional tone and text as any other form of official school communication.

Email is governed by the same rules which cover all home-school correspondence. Therefore, copies should be kept as a record of the communication e.g. by keeping a saved or printed copy, forwarding the email to the school office or other relevant staff.

Attachments which include personal details or pupils or other persons must be sent as a password protected document.

School email accounts must not be used to send, store or circulate personal email.

The sending of abusive, threatening, discriminatory or other offensive email is forbidden and may be considered a criminal act. Bear in mind that emails may be submitted as evidence in legal proceedings and that email discussions with third parties can constitute a legally binding contract.

Email attachments should be opened with care unless you have absolute confidence in its origin as this is one of the most likely points of introducing a virus into a computer system.

An individual should not access the email of another individual within the school without express permission and a clear understanding of the reason for the proxy access. However, staff should be aware that school email accounts may be accessed by other school staff for monitoring or management purposes.

Action you must take if in receipt of inappropriate emails

- It is impossible to control what information is sent to a member of staff by email. However if offensive, obscene and/or discriminatory material is received it is then the responsibility of the

receiver to report immediately, and in writing, to the designated person (Head of School/ Business Manager) in school. Never send a reply.

- Keep a printed copy of the email as evidence and pass a copy of the email to the appropriate person for the record. Ensure that the sender's information is also recorded as their email service provider may take action.

- Do not forward any email containing a 'sexting' image of a child, even for investigation purposes. It is illegal to distribute indecent images of children, even if the image was originally created by the child themselves.

Published Content & the School Web Site

- The contact details on the Website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head of School will take overall editorial responsibility for the schools' website and social media accounts and ensure that content is accurate and appropriate.

Publishing Pupils' Images & Work

- Pupil's full names will not be used anywhere on the Website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Website.

Social Networking & Personal Publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Managing Filtering

- The school will work with Enhance Academy Trust, Mint, and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Head of School.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and adopted as appropriate.

- Staff mobiles must be kept switched off, or on silent, at all times and not handled or answered during lessons or meetings, except with the permission of the Head of School. Staff must not leave the classroom during lesson time to use their mobile phones. Mobile phones may only be used in line with the Mobile Phone Policy. Any staff found using a mobile phone at any other time without permission may be subject to disciplinary action by the Governing Body. Please see our Mobile Phone Policy for further clarification. The sending of abusive or inappropriate text messages is forbidden.
- Staff will be issued with a school phone where contact with pupils or parents is required.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and General Data Protection regulations 2018.

6. Communications

Introducing the Online Safety Policy to Pupils

- Our 'Acceptable Use Policy for Early Years Pupils', 'Acceptable Use Policy for Year 1 Pupils' and 'Acceptable Use Policy for Year 2 Pupil's will be discussed with the pupils at the start of each year. (see appendix 6)
- Pupils will be informed that network and Internet use will be monitored.

Staff & the Online Safety Policy

- All staff will be given access to the School Online Safety Policy and its importance explained.

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

Enlisting Parent's Support

Parents' attention will be drawn to the School Online Safety Policy in newsletters, the school brochure and on the school Website.

Online Safety training will be available to parents and information on Online Safety at home will be issued to all parents.

Remote Learning

In the event of remote learning needing to take place, this will be agreed by the Head of School and planning discussed. Teachers are required to use Microsoft Teams or Zoom and log on using their school email address only. Parents will be responsible for monitoring the pupil's engagement on the internet during the whole of the session.

7. Policy Decisions

Authorising Internet Access

- All staff/volunteers/students must read and sign the 'Acceptable Use of the Online Safety Policy for School Staff' and 'Acceptable Use Policy for Community Users of School Computers' before using any school ICT resource.
- The school will keep a record of all staff and pupils who are granted access to the school 'Cloud'. The record will be kept up-to-date, for instance a member of staff may leave or a pupil's access be withdrawn.
- At Key Stage 1, access to the Internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- Visitors will have access to a 'guest' area of the internet only.

Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor Enhance Academy Trust can accept liability for the material accessed, or any consequences of Internet access.

- The school will audit ICT provision to establish if the Online Safety policy is adequate and that its implementation is effective.

8. Handling Online Safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Head of School.
- Complaints of a child protection nature must be dealt with in accordance with school Safeguarding procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the CEOP (Child Exploitation & Online Protection) or the Police Safeguarding Unit to establish procedures for handling potentially illegal issues.

- **Failure to Comply-** Failure to comply in any way with this policy will be considered a serious risk to health and safety and all incidents of non-compliance will be investigated by a senior member of staff.

Appendices

Appendix 1: Internet use - Possible teaching and learning activities

Appendix 2: Acceptable Use Policy of Electronic Communications Policy for School Staff

Appendix 3: Acceptable Use Policy for Community Users of School Computers

Appendix 4: Good Practice Guidance for School Staff

Appendix 5: Acceptable Use Policy for Early Years, Year 1 and Year 2 pupils

Appendix 1: Internet use - Possible teaching and learning activities

Activities	Key Online Safety issues
Creating web bookmarks to provide easy access to suitable websites.	Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.
Using search engines to access information from a range of websites.	Filtering must be active and checked frequently. Parental consent should be sought. Pupils should be supervised. Pupils should be taught what internet use is acceptable and what to do if they access material they are uncomfortable with.
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication. Pupils' full names and other personal information should be omitted. Pupils' work should only be published on 'moderated sites' and by the school administrator.
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought. Photographs should not enable individual pupils to be identified. File names should not refer to the pupil by name. Staff must ensure that published images do not breach copyright laws.
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only use applications that are managed by the Local Authority and approved Educational Suppliers.

Appendix 2

Acceptable Use of the Online Safety Policy for School Staff

I confirm that I have read and understood the Online Safety Policy and that I will use all means of electronic communication equipment provided to me by the school and any personal devices which I use for school activity in accordance with the document. In particular:

- Any content I post online (including outside school time) or send in a message will be professional and responsible and maintain the reputation of the school.
- To protect my own privacy I will use a school email address and school telephone numbers (including school mobile phone) as contact details for pupils and their parents.
- If I use any form of electronic communication for contacting pupils or parents I will use the school's system, never a personal account.
- I will only use my personal mobile phone during non-teaching time; it will be kept on silent mode during lessons except in an emergency situation with the agreement of my line manager.
- I will never use my personal mobile phone or other personal electronic equipment to photograph or video pupils.
- Taking photographs and videos will only be done with the permission of pupils and/or their parents for agreed school activities.
- I will take all reasonable steps to ensure the safety and security of school IT equipment which I take off site and will remove anything of a personal nature before it is returned to school.
- I will take all reasonable steps to ensure that all personal laptops and memory devices are fully virus protected and that protection is kept up to date.
- I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded.

I confirm I have read the Online Safety Policy and will implement the guidelines indicated. In particular:

- Confidential school information, pupil information or data which I use will be stored on a device which is encrypted or protected with a strong password. Computers will have a password protected screensaver and will be fully logged off or the screen locked before being left unattended.
- I understand that I have the same obligation to protect school data when working on a computer outside school.
- I will report immediately any accidental loss of confidential information so that the appropriate action can be taken.
- I understand that the school may monitor or check my use of IT equipment and electronic communications.

Appendix 2

Acceptable Use of Online Safety Policy for School Staff

I confirm that I have read and understood the Online Safety policy and that I will use all means of electronic communication equipment provided to me by the school and any personal devices which I use for school activity in accordance with the document.

I understand that by not following these rules I may be subject to the school's disciplinary procedures.

Name _____

Signed _____

Date _____

Appendix 3

Acceptable Use Policy for Community Users of School Computers

As a user of the school's computers I recognise that it is my responsibility to follow school procedures for the safe use of computers and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all means of electronic communication equipment belonging to the school and any personal devices which I bring into school in a responsible manner and in accordance with the following guidelines:

- I will only use the school computers for purposes related to the work I am completing in school.
- I will not use a personal device I have brought into school for any activity which might be considered inappropriate in a school.
- I will not use my personal mobile phone or other electronic equipment to photograph or video pupils.
- I will not publish photographs or videos of pupils without the knowledge and agreement of the school and the pupils.
- I will not give any personal contact details such as email address, mobile phone number or social media details to any pupil in the school. I will not arrange to video conference or use a web camera with pupils unless specific permission is given by the school.
- I will take all reasonable steps to ensure the safety and security of school IT equipment, including ensuring that any personal devices or memory devices are fully virus protected and that protection is kept up to date.
- I will report any accidental access to material which might be considered unacceptable immediately to a senior member of staff and ensure it is recorded.
- I will not download or distribute games, music or pictures from the internet for personal use (they can bring viruses with them, use up capacity and potentially breach copyright).
- I will not store personal information on the school network that uses up capacity and slows down the system e.g. personal photos.
- I will not conduct private and intimate relationships via school systems.
- I will not publish or share any information I have obtained whilst working in the school on any personal website, blog, social networking site or through any other means, unless I have permission from the school.

I understand that the school has the right to examine or delete any files that may be held on its computer system, to monitor any websites visited and emails exchanged and, if necessary, to report anything which may constitute a criminal offence.

Appendix 3

Acceptable Use Policy for Community Users of School Computers

As a user of the school's computers I recognise that it is my responsibility to follow school procedures for the safe use of computers and that I have a responsibility to ask for advice if I am not sure of a procedure.

I confirm that I will use all means of electronic communication equipment belonging to the school and any personal devices which I bring into school in a responsible manner and in accordance with these guidelines.

I understand that by not following these rules my use of school facilities may be withdrawn.

Name _____

Signed _____

Date _____

Appendix 4

Good practice guidance for school staff

1 Pay close attention to the list of misuses in section 3 because this list is for your protection and clarifies how possible disciplinary action can be avoided.

2 In communications with pupils and parents, never give out personal information which identifies your home address, phone number, mobile phone number or personal email address. Once such information is known you are open to harassment through unwanted phone calls, text messages and emails.

3 Protect your social network site by using the correct privacy settings. Make sure that personal information cannot be seen from the links to your friends' sites.

4 Do not accept pupils as friends on your personal social network site. If at all possible do not include parents as friends.

5 Avoid the use of chat rooms, instant messaging or other social networking services which are accessed socially by pupils and are not monitored by the school.

6 Always keep a copy of email communications with pupils and parents (whether sent or received) and keep a note of the dates, times and content of telephone conversations.

7 If your school laptop is used outside school for non-school activities then set up a different user account to ensure that personal or confidential data is protected. Use a strong password to protect the school laptop from unauthorised access.

8 Make sure you do not allow people to see personal or confidential school information when a computer is left unattended. Turn it off, log off and set up a password-protected screen saver to prevent unauthorised access.

9 Keep all passwords and login details strictly private and always remember to log off correctly after using the computer. Never allow anyone else to use your personal login detail as you will then be held responsible for their online activity.

10 Always use the school's digital camera or video camera for taking school related pictures and upload them onto a school computer. Once uploaded, the images should be deleted from the camera's memory. Photographs of children should not be taken home to use on a personal computer.

11 The use of hand held walkie talkies is increasing in schools. Staff using this equipment should speak professionally and respect confidentiality. Be aware that the message could be overheard at either end.

12 If you are using school electronic equipment off site then take the same level of care as you would in school. A digital camera taken off site should not be returned to school with personal photographs on it.

13 It is not recommended that personal financial transactions are made on school equipment as information may become accessible to pupils.

14 Observe sensible precautions when taking photographs which may include pupils: always obtain students and/or parental permission and make sure that individual pupils cannot be identified by name, especially if the photograph is for use on the school web site or VLE.

15 Report immediately, and in writing, to the designated person in school (or your Head of School) any web pages accessed or emails received where the content could be described as inappropriate or malicious. Keep copies as evidence.

Appendix 5

Acceptable Use Policy for Early Years Pupils

- I will take care when using the school IT equipment and use it properly
- I will only share my username or password with trusted adults
- I will tell an adult if I see anything which upsets me
- I will use a safe name and not my real name on the internet
- I will only take a photograph or video of someone if they say it is alright
- Any message I send will be polite
- I will not deliberately write anything which upsets other people
- I understand that the school may talk to my parent or carer if they are worried about my use of school IT equipment
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if it was done outside school

Appendix 5

Acceptable Use Policy for Year 1 Pupils

- I will take care when using the school IT equipment and use it properly
- I will only share my username or password with trusted adults
- I will tell an adult if I see anything which upsets me
- I will always ask before downloading from the internet or using files I have brought into school because I understand the risks from virus infections
- Any work I upload on the internet will be my own
- I will only take a photograph or video of someone if they say it is alright
- All of the messages I send will be polite
- I will not post anything online which upsets other people
- I will use a safe online name and not give away my personal information or talk to people I do not know using the internet
- I understand that the school may check my use of IT and talk to my parent or carer if they are worried about my online safety
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if it was done outside school

Appendix 5

Acceptable Use Policy for Year 2 Pupils

- I will take care when using the school IT equipment and use it properly
- I will only share my username or password with trusted adults
- I will tell an adult if I see anything which upsets me
- I will always ask before downloading from the internet or using files I have brought into school because I understand the risks from virus infections
- Any work I upload on the internet will be my own
- I will only take a photograph or video of someone if they say it is alright
- All of the messages I send will be polite
- I will not post anything online which upsets other people
- I will use a safe online name and not give away my personal information or talk to people I do not know using the internet
- I understand that the school may check my use of IT and talk to my parent or carer if they are worried about my online safety
- I understand that if I do not follow these rules I may not be allowed to use the school computers or internet for a while, even if it was done outside school