Online Safety Policy
Fulbourn Primary School

Table of Contents

Policy Document number: *FPS-POL-ONS-001*
Body reviewed and approved by:
Date adopted: *January 2026, P & R Committee*
Date for review: *January 2027*
Other information: *Based on model policy produced by the ICT Service*

Online Safety Policy

Background to this policy

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

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
- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection / GDPR Policy
- Behaviour and Anti-Bullying Policy
- School Complaints Procedure
- Whistle Blowing Policy
- Mobile Phones and other devices policy
- Social Media Policy

This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

The development of our online safety policy involved:

- The Headteacher
- The Designated Safeguarding Lead
- The Computing Subject Leader
- Cambridgeshire Local Authority Advisor (The ICT Service)
- The governor responsible for Safeguarding

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 has been shared with all staff and is readily available on the school network and website and is also available on the website for parents.

- All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As online safety is an important part of our school's approach to safeguarding, 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.

Online Safety Policy

Rationale

At Fulbourn 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 users of technology at risk within and outside the school.

The risks they may face can broadly be categorised into the 4 C's; Contact, Content, Conduct, and Commerce (Keeping Children Safe in Education 2025) 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
- Phishing or financial scams
- 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. 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 / desktops - staff devices can also be used at home in accordance with the staff Acceptable Use Policy, particularly with regard to GDPR.
- Staff have access to school systems beyond the school building (e.g. MIS systems, cloud platforms e.g. Microsoft 365 including Teams, Reachmoreparents/Weduc, Insight).
- Visualisers and Interactive Whiteboards
- Staff level internet access
- Social Media – e.g. school Facebook

Pupils:

- Curriculum laptops / iPads including filtered access to the Internet and pupil level access to areas of the school network
- Peripherals including programming resources
- Cloud platforms / online tools providing pupils with access within and beyond the school gates - EdShed or Times Tables Rockstars

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

The online safety curriculum

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.

At Fulbourn Primary School we believe that a comprehensive programme 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.

Our online safety curriculum is based on the Cambridgeshire PSHE Service Primary Personal Development Programme, supported by materials from the TEACH Computing Scheme and Project Evolve.

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
- A flexible curriculum which is able to respond to new challenges as they arise.

Use of Artificial Intelligence Tools such as ChatGPT have been proven to reduce workload for teachers and senior leaders. This is a new tool for use in schools, and whilst there are benefits, there are also risks including errors and false information. Staff must use AI with caution and fact check any outputs that are to be used when teaching the children. Please refer to our AI Policy.

Continued Professional Development

In accordance with KCSiE guidance, staff at Fulbourn Primary School receive safeguarding and child protection training at induction. This training covers online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring. Safeguarding, child protection and online safety training is regularly updated during staff meetings and through updates from the school's online safety and Designated Safeguarding Lead, as well as training from external providers where appropriate.

Fulbourn Primary School will identify a member of the senior leadership team and a governor, to be responsible for ensuring the DfE filtering and monitoring standards are met. Currently, these roles are held by Ellie Crowe (DSL) and Sarah Davies (Governor with responsibility for Safeguarding) These identified

individuals will receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.

New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.

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.

Mobile phones and use of mobile data in school

Keeping Children Safe in Education acknowledges that "many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G)." It highlights the need for schools to have a clear policy statement on, and carefully consider *"how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy."*.

The school's approach is made clear within staff and pupil Acceptable Use Policies and the Use of Mobile Phones Policy.

Monitoring and averting online safety incidents

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.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This includes

- Safeguarding Online Incident Management including real-time alerts
- Analytics platform
- Scheduled reporting
- A filtering service that is compliant with the UK Safer Internet Centre, KCSIE, the Internet Watch Foundation Block List, Prevent Duty, Home Office Terrorism Block List

For further information on safeguards built into the school's infrastructure please see information in this link: https://www.schoolsbroadband.co.uk/resources/

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
- Auto-generated alerts which flag up activity in specific safeguarding categories which may raise child protection concerns
- Use of additional reporting tools to monitor and investigate pupil use of the internet and school provided devices.

Staff use of the schools' internet is also monitored and investigated where needed.

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.
- All pupils in Years 1-6 have individual, password protected logins to the school network and our Microsoft 365 system.
- Visitors to the school can access the guest wifi network using a daily changing visitor username and password.
- Supply teachers can access part of the school systems on a school device using a supply login and password, shared by the office team.
- 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 main wireless network
- A guest wireless network is provided for staff members' personal devices and details can be 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 to an acceptable level.

Responding to online safety incidents

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, Fulbourn 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 AUPs or reporting incidents to the police and other authorities – see appendix 1: Cambridgeshire & Peterborough Safeguarding Partnership Board Procedure).

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 have 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 she 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 and it may be inadvisable to delete, save or share content. The school will always seek to resolve

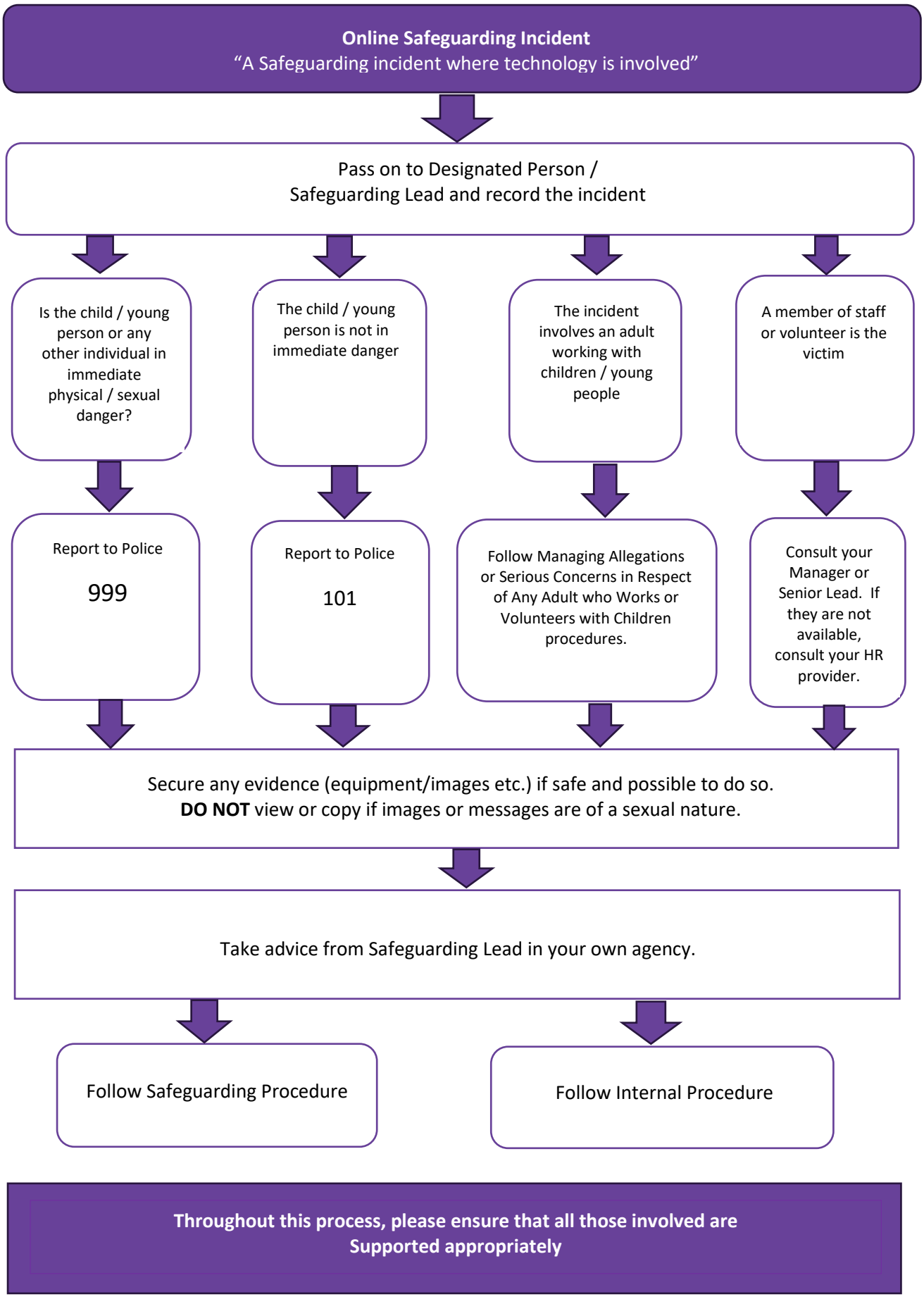
areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

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.

Appendix 1: Cambridgeshire & Peterborough Safeguarding Partnership Board Procedure

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

If you think that a child or young person is at risk of serious harm contact Children Social Care https://safeguardingcambspeterborough.org.uk/concerned/
Out of hours emergencies 01733 234724.


Online Safeguarding Incident
"A Safeguarding incident where technology is involved"
Pass on to Designated Person / Safeguarding Lead and record the incident
Is the child / young person or any other individual in immediate physical / sexual danger?
The child / young person is not in immediate danger
The incident involves an adult working with children / young people
A member of staff or volunteer is the victim
Report to Police 999
Report to Police 101
Follow Managing Allegations or Serious Concerns in Respect of Any Adult who Works or Volunteers with Children procedures.
Consult your Manager or Senior Lead. If they are not available, consult your HR provider.
Secure any evidence (equipment/images etc.) if safe and possible to do so.
DO NOT view or copy if images or messages are of a sexual nature.
Take advice from Safeguarding Lead in your own agency.
Follow Safeguarding Procedure
Follow Internal Procedure
Throughout this process, please ensure that all those involved are Supported appropriately

Appendix 2: Staff & Visitor E-Safety Acceptable Use Policy/Agreement

Contents

All staff should read and agree to abide by this document to demonstrate that they agree with the statements.

This policy covers the following aspects of e-safety in relation to all school staff:

- Use of school-based equipment
- Social Networking
- Managing digital content
- Email
- Mobile phones and devices
- Learning and teaching

School Policy

Modern technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school / academy systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable use policy agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people. I understand that the rules set out in this agreement also apply to use of these technologies out of school, and to the transfer of personal data out of school.

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 my personal 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.
- 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 seek consent from the e-safety coordinator/ headteacher prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- 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/ Headteacher/ DSL.
- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- 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 network manager/e-safety coordinator (as appropriate)
- 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.
- Wherever possible I will use school provided cloud storage solutions to move files between devices. If I have to use a portable storage device (USB sticks, SSD cards, portable hard drives etc) I will ensure that it has been approved for use on the school network by the network manager/e-safety co-ordinator.
- I will ensure that any personal or sensitive information taken off site will be stored on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.

- Any information asset, which I create or have access to from other information systems, which could be deemed as personal or sensitive will be either stored on the school network or school provided cloud storage 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 network manager/e-safety co-ordinator.
- 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 computer 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.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

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.
- I know that 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.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school or for school use.
- 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/ Home School Agreement (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 device memory.

- 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 only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will use my school email address for all email 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.
- Any personal device used to access school email or other communication systems will be encrypted and secured using a password in line with the school's password policy or biometric technology.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- I will comply with the privacy requirements of GDPR and the 2019 DPA when sending emails to groups of people by ensuring that all such emails are sent to Undisclosed Recipients.
- Emails sent to external organisations will be written carefully and if necessary, authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- I will ensure that I manage my email account and delete emails no longer required. Information I have a legitimate need to retain will not be kept in my email inbox but will be saved appropriately in the school's chosen storage system, ensuring access for other users if appropriate.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

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 school hours.
- Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances. If I have to keep Bluetooth turned on, I will ensure that the connection has a name appropriate to the setting.
- 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 and stage 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 and the use of AI generated content at all times.

Appendix 3: Key Stage 2 Acceptable Use Policy/Agreement

My Online Safety Rules

- I will only use school IT equipment for activities agreed by school staff.
- 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.
- I will not use my personal email address or other personal accounts in school when doing schoolwork.
- I will not sign up for any online service on school devices unless this is an agreed part of a school project approved by my teacher and agreed by my parent/carer.
- I will only open email attachments if it has been approved by a member of school staff in school or a parent/carer out of school. If I am unsure about an attachment, I will ask an adult for help.
- I will not tell anyone other than my parents/carers my passwords. I will not use other people's usernames or passwords to pretend to be them online.
- I will make sure that all online contact I make is responsible, polite and sensible. I will be kind and respectful at all times.
- I will not deliberately look for, save or send anything that someone could find unpleasant or upsetting. If I come across anything upsetting, unpleasant or nasty, or anything that makes me feel unsafe, I will tell my teacher or my parent/carer immediately.
- If someone says, asks or posts anything upsetting, unpleasant or nasty, about me or anything that makes me feel unsafe, I will not reply. I will tell my teacher, my parent/carer or another trusted adult immediately.
- I will not give out my own or other people's personal information such as name, phone number, home address, interests, schools or clubs. If I have to use a name online, I will use an anonymous nickname. I will tell my teacher or parent/carer if anyone asks me online for personal information.
- Uploading or sending my image (photographs, videos, live streaming) online puts me at risk. I will always seek permission from my teacher or parent/carer if I wish to do this. I will not take, share or upload any image of anyone else without their permission and also, if they are a child, without their parent's/carer's permission.
- Even if I have permission, I will not upload any images, videos, sounds or words that **could** upset, now or in the future, any member of the school community, as this is cyberbullying.
- I understand that some people on the internet are not who they say they are, and some people are not safe to be in contact with. I will not arrange to meet someone I only know on the internet. If someone asks to meet me, I will not reply to them and I will tell a teacher or a parent/carer immediately.

- I understand that everything I do or receive online can be traced now and in the future. I know it is important to build a good online reputation.
- I understand that some personal devices are allowed in school and some are not, and I will follow the rules. I will not assume that new devices can be brought into school without getting permission.
- I will not lie about my age in order to access games, apps or social networks that are for older people as this will put me at risk.
- I understand that these rules are designed to keep me safe now and in the future. If I break the rules my teachers will look into it and may:
  - Speak to me about my behaviour
  - Speak to my parents/carers about my use of technology
  - Remove me from online communities or groups
  - Not allow me to use laptops/computers or other mobile devices to access the internet, school computer network or particular programmes and apps.
  - Take any other action necessary to keep me and others safe.

Agreement

I am signing below to show that I understand and will try to abide by these rules.

Pupil's Name	
Signed	
Date	

Appendix 4: EYFS and Key Stage 1 Acceptable Use Policy/Agreement

My online Safety Rules

- I only use the internet at school when an adult is with me.
- I only click on links and buttons online when I know what they do.
- I keep my personal information safe.
- I will not share my passwords with anyone.
- I only send messages online which are polite and friendly.
- I know the school/setting can see what I am doing online.
- I always tell an adult/teacher/member of staff if something online makes me feel unhappy or worried.
- I know what might happen to me at school if I do not follow the rules
- I have read and talked about these rules with my parents/carers