Computing and Online Safety Policy

Review Date: September 2024

Next review Date: September 2025

Adopted by the Governing Body on: 23 Sep 2024

Please read this policy alongside our school Child Protection and Safeguarding Policy and other relevant policies such as Behaviour, Anti-bullying and Hate, PSHE, SEND, Teaching, Learning and Assessment, and Acceptable Use Policy. This policy is applicable to both the School and the Nursery, hereafter referred to as the school.

Review

The governing body reviews this policy annually. The governors may, however, review the policy earlier than this, if the government introduces new regulations, or if the governing body receives recommendations on how the policy might be improved.

VERIFICATION CERTIFICATE

Document Title: Issue:	Computing and Online Safety Policy 3
Reviewer: Position: Signature: Date:	Ceri Baggus Designated Safeguarding Lead  11.9.24
Approver: (on behalf of the Governing Body) Position: Signature: Date:	Nicolas Dowler Chair of Governors N.Dowler 23.09.24

DOCUMENT ISSUE/AMENDMENT HISTORY
(previous versions not numbered nor amendments noted)

Issue	Date	Amendment
1	4.10.22	Policy reviewed and updated for full Governor ratification
2	3.9.23	Policy reviewed and updated for full Governor ratification
2	11.9.24	Policy reviewed and updated for full Governor ratification any changes highlighted in red.

Contents

Introduction:

Computing in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Computing covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of information technology (IT) within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include (but are not limited to):

- Websites
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Seesaw/ Timetable Rock stars/ Numbots/ Spelling shed
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Cirencester Primary School, we understand the responsibility to educate our pupils about Online Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, Governors and visitors) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones etc.)

Keeping Children Safe in Education 2024 states that the breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images(e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying

commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Overview:

This policy aims to:

- Set out expectations for all Cirencester Primary school community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)
- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:
  - for the protection and benefit of the children and young people in their care, and
  - for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
  - for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanors will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying and Hate Policy)

Further help and support:

Internal school channels should always be followed first for reporting and support, as documented in school policy documents, especially in response to incidents, which should be reported in line with your Safeguarding Policy. The DSL will handle referrals to local authority multi-agency safeguarding hubs (MASH) and in most cases the headteacher will handle referrals to the LA designated officer (LADO). The local authority, academy trust or third-party support organisations you work with may also have advisors to offer general support.

Scope:

This policy applies to all members of the Cirencester Primary community (including teaching and support staff, supply teachers and tutors engaged under the DfE National Tutoring Programme, Governors, volunteers, contractors, students/pupils, parents/carers, visitors and community users) who have access to our digital technology, networks and systems, whether on-site or remotely, and at any time, or who use technology in their school role.

Roles and Responsibilities

This school is a community and all members have a duty to behave respectfully online and offline, to use technology for teaching and learning and to prepare for life after school, and to immediately report any concerns or inappropriate behaviour, to protect staff, pupils, families and the reputation of the school. We learn together, make honest mistakes together and support each other in a world that is online and offline at the same time.

The Senior Leadership Team and Governors are updated by the Online Safety lead, at times via the headteacher, and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

As Online Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named Online Safety lead in our school is Mrs Katie Clissold who has been designated

this role as part of the computing lead responsibilities and Mrs Ceri Baggus is the school's designated safeguarding lead. All members of the school community have been made aware of who holds this post. It is the role of the Online Safety lead to keep abreast of current issues and guidance through maintaining a working knowledge of the responsibilities outlined in Keeping Children Safe in Education 2024 and also through the guidance of organisations such as Gloucestershire Local Authority, CEOP (Child Exploitation and Online Protection) and Childnet.

This policy, supported by the school's acceptable use agreements for staff, Governors and visitors (appendices), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child protection and Safeguarding, Health and Safety, Home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy and PSHE.

Handling online safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing, PSHE/RSHE and Citizenship). General concerns must be handled in the same way as any other safeguarding concern; safeguarding is often referred to as a jigsaw puzzle, so all stakeholders should err on the side of talking to the online-safety lead / designated safeguarding lead to contribute to the overall picture or highlight what might not yet be a problem.

Support staff will often have a unique insight and opportunity to find out about issues first in the playground, corridors, toilets and other communal areas outside the classroom (particularly relating to bullying and sexual harassment and violence).

School procedures for dealing with online-safety will be mostly detailed in the following policies (primarily in the first key document):

- Child Protection and safeguarding policy
- Child on Child Abuse Policy
- Anti-Bullying and Hate Policy
- Behaviour Policy (including school sanctions)
- Acceptable Use Policy
- Code of Conduct (employees)
- Data Protection Policy, agreements and other documentation (e.g. privacy statement and consent forms for data sharing, image use etc)

This school commits to take all reasonable precautions to ensure online safety, but recognises that incidents will occur both inside school and outside school (and that those from outside school will continue to impact pupils when they come into school or during extended periods away from school). All members of the school are encouraged to report issues swiftly to allow us to deal with them quickly and sensitively through the school's escalation processes.

Any suspected online risk or infringement should be reported to the online safety lead / designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. Any concern/allegation about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the complaint is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer). Staff may also use the NSPCC Whistleblowing Helpline.

The school will actively seek support from other agencies as needed (i.e. the local authority, LGfL, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, IWF). We will inform parents/carers of online-safety incidents involving their children, and the Police where staff or pupils engage in or are subject to behaviour which we consider is particularly disturbing or breaks the law (particular procedures are in place for the sharing of consensual or non-consensual nude/semi-nude images and/or videos and upskirting; see section below).

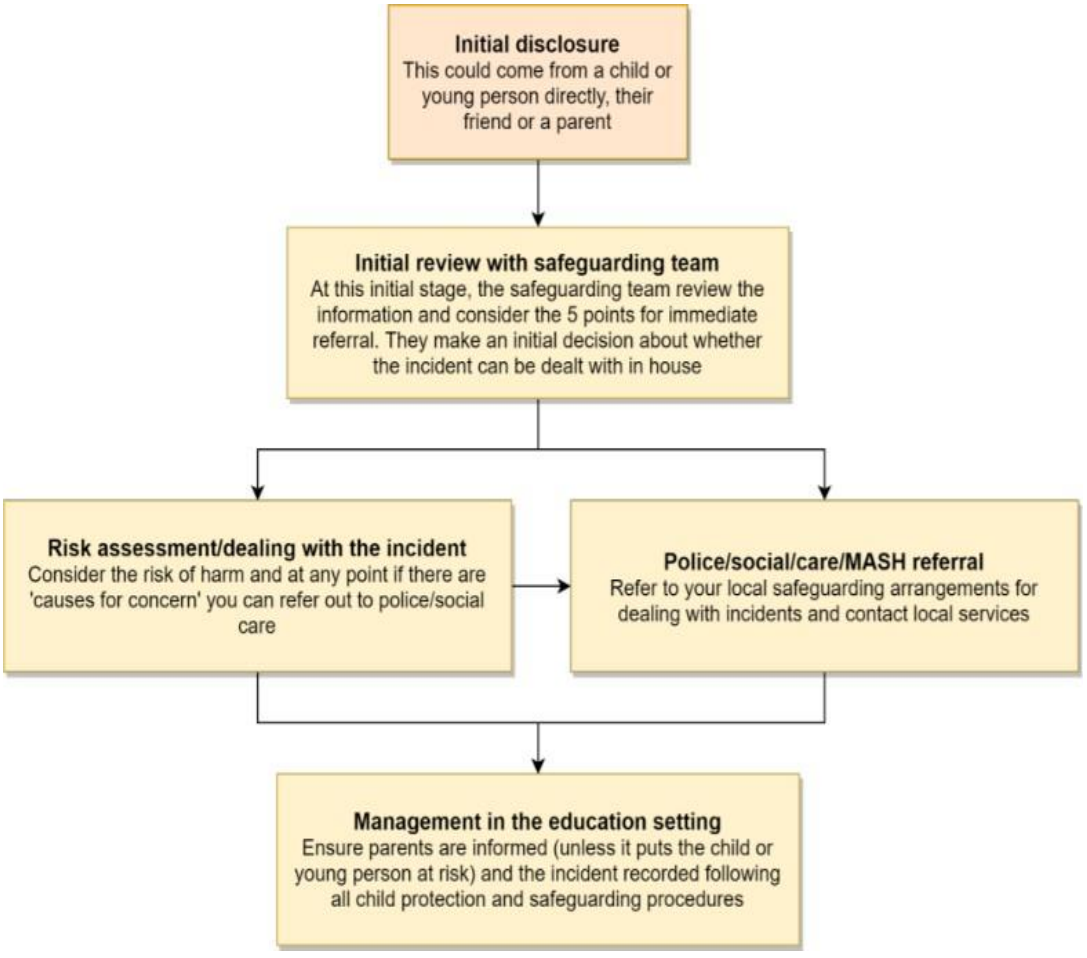
The school should evaluate whether reporting procedures are adequate for any future closures or

lockdowns/isolation etc and make alternative provisions in advance where these might be needed.

Sharing of consensual or non-consensual nude/semi-nude images and/or videos

All schools (regardless of phase) should refer to the updated UK Council for Internet Safety (UKCIS) guidance on the sharing of consensual or non-consensual nude/semi-nude images and/or videos (Sharing nudes and semi-nudes: advice for education settings) to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse. There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken. Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL.

The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes: advice for education settings to decide next steps and whether other agencies need to be involved.



It is important that everyone understands that whilst sharing of consensual or non-consensual nude/semi-nude images and/or videos is illegal, pupils/students can come and talk to members of staff if they have made a mistake or have a concern related to this.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence, as highlighted in Keeping Children Safe in Education 2024 and that pupils/students can come and talk to members of staff if they have made a mistake or have a concern related to this.

Bullying

Cyberbullying should be treated like any other form of bullying and the school's Anti-bullying and Hate policy should be followed for incidents related to cyberbullying, including issues arising from banter. Please see our Anti-bullying and Hate policy and Child on Child abuse policy for more information on prevention in the curriculum as well as how disclosures of cyberbullying are recorded and resolved.

Child on Child sexual violence and sexual harassment

DfE guidance on sexual violence and harassment is part 5 of Keeping Children Safe in Education 2024, and covers the immediate response to a report and confidentiality as well as a case study section which provides a helpful overview of some of the issues which may arise. All staff and governors are expected to read Part 5 of KCSiE24 so they have a thorough knowledge of this area of safeguarding.

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance. Staff should work to foster a zero-tolerance culture. The guidance stresses that schools must take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. The document makes specific reference to behaviours such as bra-strap flicking and the careless use of language.

Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

These are defined in the relevant Acceptable Use Policy as well as in this document, for example in the sections relating to the professional and personal use of school platforms/networks/clouds, devices and other technology, as well as to BYOD (bring your own device) policy.

Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct policy. It will be necessary to reinforce these as usual at the beginning of any school year but also to remind pupils that **the same applies for any home learning** that may take place in future periods of absence/ closure/quarantine etc.

Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Online Safety in the Curriculum

The following subjects have the clearest online safety links (see the relevant role descriptors above for more information):

- Relationships education, relationships and sex education (RSE) and health (also known as RSHE or PSHE)
- Computing

However, as stated in the role descriptors above, it is the role of all staff to identify opportunities to thread online safety through all school activities, both outside the classroom and within the curriculum, supporting curriculum/stage/subject leads, and making the most of unexpected learning opportunities as they arise (which have a unique value for pupils)

Whenever overseeing the use of technology (devices, the internet, new technology such as augmented reality, etc) in school or setting as homework tasks, all staff should encourage sensible use, monitor what pupils/students are doing and consider potential dangers and the age appropriateness of websites (ask your DSL what appropriate filtering and monitoring policies are in place).

Equally, all staff should carefully supervise and guide pupils when engaged in learning activities involving online technology (including, extra-curricular, extended school activities if relevant and remote teaching), supporting them with search skills, critical thinking (e.g. fake news), age appropriate materials and signposting, and legal issues such as copyright and data law.

At Cirencester Primary, we recognise that online safety and broader digital resilience must be thread throughout the curriculum and that is why we are working to adopt the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety) framework more closely in its key areas of Self-image and Identity, Online relationships, Online reputation, Online bullying, Managing online information, Health, Wellbeing and lifestyle, Privacy and security, and Copyright and ownership.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends.

Staff and pupils are regularly reminded of the need for password security and the secure locking of devices when not in use.

- All users read and sign an Acceptable Use Agreement at the beginning of each key stage to demonstrate that they have understood the school's Online safety Policy.
- Pupils are not allowed to deliberately access online materials or files on the school network of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this to the Computing Lead, IT technician or Business Manager.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended in a logged-on state.
- In our school, all computing password policies are the responsibility of the IT technician and Business Manager and all staff and pupils are expected to comply with the policies at all times.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the **South West Grid for Learning** (SWGfL) is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up. The designated safeguarding lead has ultimate responsibility for overseeing and understanding the filtering and monitoring systems and processes in place in school.

The school maintains students will have supervised access to Internet resources (where reasonable) through the school's internet technology. However, with the internet of things being everywhere it is impossible for staff to continuously monitor their access.

- Staff will preview any sites which pupils will use before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

Infrastructure

- School internet access is controlled through the LA's web filtering service.
- Cirencester Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998 and General Data Protection Regulation (GDPR) 2018.
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the nearest member of staff and to one of the safety leads as soon as possible.
- Pupils and Staff using personal **encrypted** removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to- date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media it must be given to the teacher for a virus check first.
- Pupils and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Computing Lead or IT Technician.
- The Designated Safeguarding Lead (DSL) is responsible for internet security and filtering.

Managing other Web 2 technologies

Web 2, including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils and staff to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

- At present, the school endeavors to deny access to social networking sites to pupils within school.
- Staff must ensure that any online activity (including use of social media), both in school and outside school, will not bring their professional role into disrepute.
- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Staff are expected to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).
- Our pupils and staff are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.
- Pupils and staff are encouraged to be wary about publishing specific and detailed private thoughts online.
- Our pupils and staff are asked to report any incidents of bullying to the school.

Managing the school Online Safety messages

- We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The Online safety policy will be introduced to the pupils at the start of each school year. Online safety advice is displayed in the Computer room.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, tablets, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately:

Personal Mobile devices (including phones)

- The school allows staff and parent volunteers to bring in secure (password locked) personal mobile phones and devices for their own personal use. Mobile phones must not be used in view of the children unless permission has been agreed by a member of SLT. Mobile phones must not be used and shared in any way with the children. The staff room has been designated a 'safe place' for members of staff to use their devices.
- In emergencies the school does allow a member of staff to contact a pupil or parent/ carer using their personal device. If this occurs school has advised that they set their phone number to private so ensure parents/carers don't have access to their telephone number.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device and that these devices are not used or shared with the children in any way unless under direct supervision from an SLT member.
- Pupils are not allowed to bring personal mobile devices/phones to school. In certain circumstances pupils may be given permission to have a mobile device in school, due to walking home alone. In these cases pupils hand their mobile phone into their class teacher on arrival and collect it before leaving school in the afternoon. Mobile phones are kept securely in classrooms during the school day. The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- If any illegal or inappropriate content is discovered on a device whilst on the school property, it must be taken from the individual and locked in the safe, in the office. The DSL will be informed and they will contact GCC for advice on how to move forwards. If the images are deemed graphic enough then DSL will contact the police.

School provided Mobile devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.

Managing email

The use of email within most schools is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good 'etiquette'.

- The school gives all staff their own email account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed. This account must be used for all data relating to the fulfilment of our role as educators. This also includes Governors.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. Emails which contain personal information should not be sent unless encrypted first.
- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. All children use a class or group email address.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission. Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.
- Staff must inform the Online Safety lead/line manager/IT technician if they receive an offensive e-mail.
- Pupils are introduced to email as part of the Computing Scheme of Work.

Safe Use of Images Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

Publishing pupils' images and work

All parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- recorded/ transmitted on a video or webcam
- in display material that may be used in the school's communal areas. This will not include personal data relating to the individuals, which is easily attributed.
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
- School Instagram page

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/carers may withdraw permission, in writing, at any time.

Pupils' surnames will not be published by the school alongside their image and vice versa. Local press may insist on publishing photographs with full details of children. Permission for the press to publish these photographs must come from parents at all times.

E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Misuse and infringements

Complaints

Complaints relating to Online Safety should be made to the Online Safety lead or DSL. Incidents should be logged and follow-up action taken by the Online Safety lead.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Online Safety lead.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Online Safety lead, depending on the seriousness of the offence; investigation by the headteacher, (DSL) LA, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Equal Opportunities

Cirencester Community Primary School strives to ensure that the culture and ethos of the school are such that, whatever the heritage and origins, abilities and needs of members of the school community, everyone is equally valued and treats one another with respect. All pupils have the right to be given opportunities and access to the full curriculum regardless of ethnicity, gender, social circumstances, ability, disability, age, nationality or citizenship. Pupils should be provided with the opportunity to experience, understand and celebrate diversity.

Inclusion

The school provides effective learning opportunities for all pupils. When planning, teachers set high expectations and provide opportunities for all pupils to achieve. All teachers are aware that pupils bring to school different experiences, interests and strengths, which will influence the way they learn. Teachers plan their approach to teaching and learning so that all pupils can take part in lessons fully and effectively. Specific action is taken to enable the effective participation of pupils with disabilities. All children should receive high quality computing and online safety lessons and teaching.

Pupils with additional needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid the establishment and future development of the schools' Online Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of Online Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of Online Safety. Internet activities are planned and well managed for these children and young people. SEND version of Acceptable use policy is available for children who require.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting Online Safety both in and outside of school. We aim to regularly consult and discuss Online Safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

Parents/ carers are required to make a decision as to whether they consent to images of their child

being taken/ used in the public domain (e.g. on school website).

The school disseminates information to parents relating to Online Safety where appropriate in the form of;

- Information and celebration evenings
- Posters
- Website postings
- Newsletter items
- Emails
- Parent Texts

Writing and Reviewing this Policy Review Procedure

There will be an on-going opportunity for staff to discuss with the Online Safety coordinators any issue of Online Safety that concerns them. This policy will be reviewed annually and consideration given to the implications for future whole school development planning. The policy will be amended if new technologies are adopted or Central Government changes the orders or guidance in any way.

Appendix 1
Cirencester Primary School
Acceptable Use Agreement:
KS1 Pupils

For pupils to read and sign when they begin with the school and all pupils at the start of Year 1.

My name is _____

To stay **SAFE online and on my devices**, I follow the Digital 5 A Day and:

1. I only **USE** devices or apps, sites or games if a trusted adult says so
2. I **ASK** for help if I'm stuck or not sure
3. I **TELL** a trusted adult if I'm upset, worried, scared or confused
4. If I get a **FUNNY FEELING** in my tummy, I talk to an adult
5. I look out for my **FRIENDS** and tell someone if they need help
6. I **KNOW** people online aren't always who they say they are
7. Anything I do online can be shared and might stay online **FOREVER**
8. I don't keep **SECRETS** or do **DARES AND CHALLENGES** just because someone tells me I have to
9. I don't change **CLOTHES** or get undressed in front of a camera
10. I always check before **SHARING** personal information
11. I am **KIND** and polite to everyone

My trusted adults are:

_____ **at school**

_____ **at home**

Draw a picture of your trusted adults .

Appendix 2
Cirencester Primary School
Acceptable Use Agreement:
KS2 Pupils

For pupils to read and sign when they begin with the school and at the beginning of Year 3.

These statements can keep me and others safe and happy at school and at home.

1. ***I learn online*** – I use the school's internet, devices and logins for schoolwork, homework and other activities to learn and have fun. All school devices and systems are monitored, including when I'm using them at home.
2. ***I ask permission*** – At home or school, I only use the devices, apps, sites and games I am allowed to and when I am allowed to.
3. ***I am creative online*** – I don't just spend time on apps, sites and games looking at things from other people. I get creative to learn and make things, and I remember my Digital 5 A Day.
4. ***I am a friend online*** – I won't share or say anything that I know would upset another person or they wouldn't want shared. If a friend is worried or needs help, I remind them to talk to an adult, or even do it for them.
5. ***I am a secure online learner*** – I keep my passwords to myself and reset them if anyone finds them out. Friends don't share passwords!
6. ***I am careful what I click on*** – I don't click on unexpected links or popups, and only download or install things when I know it is safe or has been agreed by trusted adults. Sometimes app add-ons can cost money, so it is important I always check.
7. ***I ask for help if I am scared or worried*** – I will talk to a trusted adult if anything upsets me or worries me on an app, site or game – it often helps. If I get a funny feeling, I talk about it.
8. ***I know it's not my fault if I see or someone sends me something bad*** – I won't get in trouble, but I mustn't share it. Instead, I will tell a trusted adult. If I make a mistake, I don't try to hide it but ask for help.
9. ***I communicate and collaborate online*** – with people I already know and have met in real life or that a trusted adult knows about.
10. ***I know new online friends might not be who they say they are*** – I am careful when someone wants to be my friend. Unless I have met them face to face, I can't be sure who they are.
11. ***I check with a parent/carer before I meet an online friend*** the first time; I never go alone.
12. ***I don't do live videos (livestreams) on my own*** – and always check if it is allowed. I check with a trusted adult before I video chat with anybody for the first time.
13. ***I keep my body to myself online*** – I never get changed or show what's under my clothes when using a device with a camera. I remember my body is mine and no-one should tell me what to do with it; I don't send any photos or videos without checking with a trusted adult.

14. ***I say no online if I need to*** – I don't have to do something just because someone dares or challenges me to do it, or to keep a secret. If I get asked anything that makes me worried, upset or just confused, I should say no, stop chatting and tell a trusted adult immediately.
15. ***I tell my parents/carers what I do online*** – they might not know the app, site or game, but they can still help me when things go wrong, and they want to know what I'm doing.
16. ***I follow age rules*** – 13+ games and apps aren't good for me so I don't use them – they may be scary, violent or unsuitable. 18+ games are not more difficult but very unsuitable.
17. ***I am private online*** – I only give out private information if a trusted adult says it's okay. This might be my address, phone number, location or anything else that could identify me or my family and friends; if I turn on my location, I will remember to turn it off again.
18. ***I am careful what I share and protect my online reputation*** – I know anything I do can be shared and might stay online forever (even on Snapchat or if I delete it).
19. ***I am a rule-follower online*** – I know that apps, sites and games have rules on how to behave, and some have age restrictions. I follow the rules, block bullies and report bad behaviour, at home and at school.
20. ***I am not a bully*** – I do not post, make or share unkind, hurtful or rude messages/comments and if I see it happening, I will tell my trusted adults.
21. ***I am part of a community*** – I do not make fun of anyone or exclude them because they are different to me. If I see anyone doing this, I tell a trusted adult and/or report it.
22. ***I respect people's work*** – I only edit or delete my own digital work and only use words, pictures or videos from other people if I have their permission or if it is copyright free or has a Creative Commons licence.
23. ***I am a researcher online*** – I use safe search tools approved by my trusted adults. I know I can't believe everything I see online, know which sites to trust, and know how to double check information I find. If I am not sure I ask a trusted adult.

~~~~~~~~~~~~~~~~~~~~~

I have read and understood this agreement.

If I have any questions, I will speak to a trusted adult: at school that includes

_____

Outside school, my trusted adults are_____

I know I can also get in touch with Childline

Signed:_____ **Date:**
~~~~~~~~~~~~~~~~~~~~~

Appendix 3

5 SMART Rules

There are lots of resources online to help you as well as the following 5 SMART Rules for primary aged children.

Safe:

Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.

Meet:

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time

Accepting:

Accepting emails, messages, opening files, images or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

Reliable:

Someone online might lie about who they are and information on the internet may not be true. Always check information by looking at other websites, in books, or with someone who knows. If you are going to chat online it's best to only chat to your real world friends and family.

Tell:

Tell a parent, carer or a trusted adult if someone, or something, makes you feel uncomfortable or worried, or if you or someone you know is being bullied online. **For more information, take a look at these online resources:** http://www.childnet.com/ufiles/Supporting-young-people- online.pdf https://www.thinkuknow.co.uk/parents/Support-tools/How-to- guides/ https://www.thinkuknow.co.uk/

https://www.saferinternet.org.uk/

https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/e- safety-schools/