Steeple Morden C of E (VC) Primary School

Online Safety Policy

"I was lost, but now I am found", Luke 15:24

1. Introduction and Scope of this Policy

1.1 Our Online-Safety Policy aims to recognise the role ICT has in the light of the Every Child Matters 'staying safe' outcome. ICT (information and communications technology - or technologies) is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning. Online safety is not primarily an ICT or computing issue, but relates directly to child safety and is an extension of safeguarding procedures. The DFE's statutory guidance 'Keeping Children Safe in Education was revised in 2024 and specific references to online safety is made throughout. Therefore, this policy should be read in conjunction with those for Anti-Bullying, Safeguarding & Child Protection, ICT, Data Protection, PSHE, RSE and Safer Care of Conduct.

1.2 Protecting our pupils, staff and governors properly means thinking beyond the traditional school environment. Safeguarding our children in the real and virtual world is everyone's responsibility, including all staff, students / pupils, volunteers, parents / carers, visitors, and community users.

1.3 The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / 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 covered by this policy, which may take place out of school, but is linked to membership of the school.

1.4 The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate safety behaviour that take place out of school.

2. Technologies

2.1 Technology has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging communication tools used in school and, more importantly in many cases, used outside of school by children may include:

- The Internet
- Virtual Learning Environments (VLE) or Learning Platforms
- E-mail
- Instant messaging, such as WhatsApp often using web cams/live-streaming. Live video platforms such as Zoom and FaceTime, where children speak with friends and family and take part in educational events
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites e.g. www.facebook.com, www.twitter.com, Instagram
- Video broadcasting sites e.g. http://www.youtube.com/, TikTok and twitch, enable anyone to view, create live streams or upload self-created video content either pre-recorded or in real time.
- Chat Rooms - written communication between users, with the potential for misinterpretation
- Gaming Sites and voice/video communication with known/unknown users within games such as Roblox and Minecraft
- Music download sites e.g. http://www.apple.com/itunes/

- Mobile phones with internet, e-mail, camera and video functionality. Allow access to apps such as Instagram and Snap chat.
- Kindles and iPods (although not their primary use, these can allow access to the internet)
- Internet of things (The Internet of things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data e.g. talking toy bears which search the internet for response, smart metres, Amazon's voice activated Alexa).

2.2 Additionally, the range of devices with which these communication tools can be accessed are varied, and may include laptops, desktop PCs, mobile/smart phones, games consoles, TVs, watches, tablet computers, and cameras (with WiFi capability).

3. Teaching and Learning

3.1 The National Curriculum 2014 requires children to be responsible, competent and confident users of ICT. Internet use is a part of the curriculum we provide in our school and a necessary tool for staff, pupils and governors. Therefore, it is important everybody is aware of what is safe and acceptable use. This will be taught to pupils as an integral part of lessons where the Internet is used and embedded within the day-to-day use of the Internet on the school site.

3.2 In delivering the curriculum, teachers will plan for and make use of communications technology, for example, web-based resources such as Mathletics. Access to life-long learning and employment increasingly requires computer and communications use and pupils need to develop life skills in their safe use.

3.3
DfE Guidance, referenced in Keeping Children Safe in Education 2024 (135) states:

The breadth of issues classified within online safety is considerable and ever evolving, 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:** 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, and*

***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/).*

3.31 Pupils will be taught:

- How to interact positively and harness the potential of the internet but also to recognise and to be aware of the risks and social pressures when online;
- Strategies for protecting themselves and others (against these risks when supported or unsupported by adult supervision, for example that they know to inform a trusted adult (e.g. teacher/parent) immediately if they encounter any material or individuals that makes them feel uncomfortable or upset;
- To acknowledge the source of information, when using Internet material for their own use;
- How to think critically about the content they see (including 'fake news' and digitally manipulated images) and the people they interact with online through discussion and mocked-up examples e.g. that the writer of an e-mail or the author of a Web page might not be the person claimed.
- How to validate information before accepting that it is necessarily accurate;
- How to report online bullying or content

- How to protect themselves from other online situations that could affect their mood and emotions (see 'Life in Likes' Children's Commissioner report into social media use among 8-12 year olds)
- To develop an awareness of the risks how games can have the potential to lead to risk taking habits such as 'skin gambling' and how games may try to get them to spend real money
- SEND pupils face additional risks online – provision is made for these pupils and their parents and carers directed to support and offered advice. *Any reports of abuse involving children with SEND will therefore require close liaison with the designated safeguarding lead (or a deputy) and the special educational needs coordinator (SENCO) or the named person with oversight for SEND…(KCSIE 2024 203)*

3.4 We will use available resources to engage children actively in learning about online-safety. This includes use of resources from the ICT Education Service (LA), Project Evolve https://projectevolve.co.uk/ and CEOP's resources such as the thinkuknow and childnet websites, government publications from the DfE (Last updated January 2023) which outlines how schools can ensure pupils understand how to stay safe online https://www.gov.uk/government/publications/teaching-online-safety-in-schools and other suitable material sourced by teachers to support teaching points in lessons. Other initiatives in school are linked to our PSHE curriculum, including Anti-bullying week, and Online-Safety focus weeks. Online safety education traverses the curriculum however, explicit teaching of areas of online safety are clearly mapped between Computing and PSHE subjects to ensure coverage.

3.5 Parents and carers will be made aware through news letters and the year ahead meetings at the beginning of the year how they can access resources such as those offered by the safer internet centre and CEOP (Child Exploitation and Online Protection Command) to help them talk to their child about their internet use and technical advice such as how to set up effective parental controls offered by their internet service providers.

3.6 Staff will receive training annually around their safe use of technology and how to conduct themselves online and what do to if they are the target of online abuse. In line with advice from Keeping Children Safe in Education 2020, all staff will be made aware that 'upskirting' is now a criminal offence. A definition has been included which describes upskirting as, "taking a picture under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks to obtain sexual gratification, or cause the victim humiliation, distress or alarm" (DfE, 2020a)"

4. Technology and Infrastructure Management

4.1 Everyone in our school community is responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Keeping Children Safe in Education - September 2024 (133) states "Whilst it is essential that governing bodies and proprietors ensure that appropriate filtering and monitoring systems are in place, they should be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regard to online teaching and safeguarding.".

a) School ICT systems will be managed in ways that ensure the school meets the online-safety technical requirements outlined in any relevant Local Authority Online-Safety Policy and guidance, including system security arrangements.
b) There will be regular reviews and audits of the safety and security of school ICT systems;
c) Servers, wireless systems and cabling will be securely located, password protected and physical access restricted;
d) All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the ICT Technician and will be reviewed annually by the ICT Technician and ICT Co-ordinator;
e) All users will be provided with a secure username and password by the ICT Co-ordinator (for pupils) or the Bursar (Staff and visitors) who will keep an up-to-date record of users and their usernames. Staff users will be required to change their password every 90 days. If required, a username and password will be provided to supply or visiting teachers by the Bursar;
f) All pupils will be given a class login that relates to their year of entry to school;

g) The "master / administrator" passwords for the school ICT system, used by the ICT Technician and Computing Co-ordinator are shared with the Headteacher and the Bursar, and kept in a secure place (in an encrypted digital file and a print-out is stored securely);

h) All users are responsible for the security of their username and passwords, must not allow other users to access the systems using their log on details, and must immediately report any suspicion or evidence that there has been a breach of security;

i) School staff and LA ICT technical staff can, and do, regularly monitor and record the activity of users on the school ICT systems and users are made aware of the capacity to monitor use in the Acceptable Use Policy (Appendix 1 & 2);

j) Remote management tools are used by our ICT Technician and the LA ICT technical staff to control workstations and view users activity;

- All safeguarding issues must immediately be reported to the designated person for Child Protection through the appropriate Safeguarding procedure. The DSL (Designated Safeguarding Lead) has overall responsibility for safeguarding and child protection, including online safety, responding to reports of child-on-child abuse even if it happens offsite, and understanding the filtering and monitoring systems and processes in place; they can be supported by appropriately trained deputies and should liaise with other staff as appropriate, but this responsibility cannot be delegated.
- An appropriate system is in place for users to report any actual / potential online-safety incident to the ICT Technician or Computing Co-ordinator;

k) Appropriate security measures are in place (through Sophos Protection software, provided by the LA) to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc. from accidental or deliberately malicious attempts which might threaten the security of the school systems and data (including virus protection); The ICT Technician. We know these are effective because the school holds a current certificate from smoothwall, who provide the filtering for the school. The ICT technician will ensure this is kept up-to-date see also 5.73.

l) Executable Files: These are files that can install, run or download programs on a computer. Permission to run these should be sought from the ICT Technician or the ICT Co-ordinator. This includes permission to install new software from an online download or directly from other media (CD-Rom/USB Flash Drive) onto school provided equipment whether on or off site (e.g. at teachers working at home);

m) Pupils will not normally be permitted to remove ICT equipment from school to use at home. Permission from the Headteacher must be sought and a written agreement signed by the Headteacher and the child's parents/carers;

n) Personal use of school provided ICT equipment by anyone other than staff is strictly forbidden. Use by their family members is also strictly forbidden;

o) Before using personal ICT equipment in school (such as a tablet device), staff should seek permission from the ICT Technician and/or ICT Co-ordinator to ensure that it is compatible with our ICT security systems. It must also comply with any Health & Safety requirements (e.g. electrical safety testing for mains powered devices);

p) The use of removable media (e.g. memory sticks / CDs / DVDs) to store data by users on school ICT equipment is actively discouraged, though it is recognised that it is sometimes necessary for staff to use removable media when transferring files from one device to another. It is not permitted for pupils to use removable media to store data with school ICT equipment. Any staff use of removable media must therefore be in accordance with the Acceptable Use Policy (Appendix 1 & 2) devices will be scanned for viruses;

q) Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured (the LA provided email address for school staff is encrypted and as secure as can be reasonably expected).

5. Managing Internet Access

5.1 Cambridgeshire LA, through The ICT Service, will provide filtered internet access. The filter which will deny access to inappropriate sites and provides a facility to quickly report any inappropriate sites not already blocked.

5.2 To ensure safe Internet access:

a) All members of the school community who have access to ICT equipment, whether or not that equipment is Internet enabled, will be required to read and agree to by signing an Acceptable User Policy (Appendix 1 & 2) agreement (See Appendices 1 and 2);
b) Access will be granted to pupils as part of classroom activities after some education in internet use and internet safety;
c) Pupils will be informed that their internet use will be supervised and monitored;
d) Pupils will not be allowed to access public chat rooms;
e) Parents will be informed that pupils will have supervised internet access (through the pupil Acceptable Use Policy, see Appendix 1);
f) The school will work in partnership with parents, the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved;
g) Staff will be informed that their internet access onsite or use of school equipment to access the internet off site can and may be periodically monitored by the ICT Technician and SMT;
h) The difference between filtering and monitoring: these two terms tend to be used interchangeably but they are different, and it is important that schools understand this and have both effective filtering and monitoring in place to adhere to the guidance.
i) Filtering restricts the content a user can access on the internet and works by blocking access to predetermined websites or web searches that contain specific words or phrases. Filtering usually operates at the perimeter of the school network, like a sieve over the school's broadband connection as data enters or leaves the building. The vast majority of Cambridgeshire schools benefit from Smoothwall filtering as part of their EastNet internet connection.
j) Monitoring, rather than intercepting data at the perimeter level, typically operates at a local level on individual devices. Monitoring systems look out for pre-set words and phrases across all user activity, not just when using the internet – for example the words typed into emails, Word or Teams chat. Safeguarding alerts are raised when these trigger words are picked up by the monitoring system and dealt with accordingly. Termly checks are jointly by ICT technician and computing co-ordinator to ensure that the filtering methods are effective in practice, these checks are and any resulting actions, are documented by the computing coordinator. The Head teacher and ICT Technician will need to be aware when this is being done; the Head and the computing coordinator have access to Smoothwall's 'Portal' allowing monitoring of devices using the school wifi through user generated reports..
k) Any problems arising from the filtering are to be reported to the ICT Technician and/or Computing Co-ordinator who will speak with The ICT Service who will advise weather they will deal with the issue or if the school needs to liaise with Smoothwall.
l) New software and hardware facilities e.g. Video conferencing, will be thoroughly tested before pupils are given access.

5.3 E-mail

5.31 Staff & Governors are expected to use only the provided email account for all school related communication (i.e. for staff and email address ending in @steeplemorden.cambs.sch.uk or for governors @smpsgovernor.co.uk.) More detailed information on how the school community will use email can be found in the appropriate Acceptable Use Policy (Appendix 1 & 2).

5.32 Where personal email is used by staff, governors or visiting/supply teachers (for example when forwarding resources or planning documents from a separate source), then it is used within strict adherence to the Acceptable Use Policy (Appendix 1 & 2) and no Protected or Restricted information held by the school, which includes individual or personal information about children in our care, will be transmitted or distributed.

5.4 Published content and the school website

5.41 The contact details on the Web site should be the school address, e-mail and telephone number. Staff lists and, where suitable, staff contact information (e.g. a teacher's email address) may be published. Personal information about volunteers or pupils will not be published.

5.42 The Headteacher and Webeditor will take overall editorial responsibility and ensure that content is accurate and appropriate; though it is expected that teaching staff will have an editorial responsibility for their class areas of the website.

5.43 We have a permanent page on the school website (under the Safeguarding tab) with links to resources to help parents manage their child's digital life. https://www.steeplemorden.cambs.sch.uk/e-safety

5.5 Publishing pupils' images and work on external websites

5.51 We celebrate the work and activities of all our pupils by carefully selecting work to be included on our school website and in the STAR (the school newspaper which is published publicly online). From time to time this work may be also published on external websites (such as the local media).

5.52 Photographs that include pupils will be selected carefully and will comply with the school's Use of Images and Visual Media Policy (see section 8). This states they will not generally include the pupils' names, they will be taken with due consideration to modesty, and they will only be used when written permission (through the Registration and General Consent forms) has been granted for the pupils pictured.

5.6 Social networking and personal publishing

5.61 Staff and volunteers will be expected to comply with the school's Safer Care Code of Conduct Policy regarding personal or social contact with pupils.

5.62 Pupils will be advised never to give out personal details of any kind which may identify them or their location.

5.63 Pupils and parents will be advised that the use of social network spaces (such as Facebook, Skype, YouTube, Instagram) is very often, at a minimum, of those over age 13 therefore is inappropriate for primary aged pupils and use of such spaces are considered by the school to be a potential Safeguarding concern and would be referred to the designated person for Child Protection in school. A survey by the BBC's news programme for children, Newsround, in February 2017 found that more than three-quarters of younger children at primary-leaving age were using at least one social media network. For 13 to 18-year-olds, 96 percent used social media networks.

5.64 Children will be encouraged to THINK before they post anything online.

T = Is it True?
H = Is it Helpful?
I = Is it inspiring?
N = Is it Necessary?
K = Is it Kind?

5.65 Increasingly, young children are using phones, and tablets to create photos and videos and share them online. Whilst this can be fun, sharing images can also be risky. It's important pupils understand what's ok to share and what they should discuss with their/parent carer first.

5.66 The Professionals Online Safety Helpline was set up in 2011 to help the children's workforce with online safety issues. The help with any online safety issues - privacy, online reputation, gaming, grooming, cyberbullying, sexting, fraud, unsolicited content, inappropriate behaviour on social media, extortion, illegal content, online rationalization, eating disorders, self-harm, online harassment and other concerns linked to the internet.

5.67 If anyone (including children/parents/ all staff) are worried about something that has happened to themselves or others online incidents can be reported to The Child Exploitation and Online Protection Centre (CEOP) works across the UK tackling child sex abuse and providing advice for parents, young people. Parents/staff can also seek advice from. https://www.thinkuknow.co.uk/parents/articles/Has-your-child-shared-a-picture-or-video-online-/

5.7 Managing filtering

5.71 The school Internet access is provided by EastNet, The ICT Service uses the web-filtering solution 'Smoothwall' filtering platform. It is designed expressly for pupils and schools. It includes filtering appropriate to the age of our pupils.

5.72 If staff or pupils discover an unsuitable site, it must be reported to the Computing Co-ordinator and/or another appropriate person such as the Deputy/Safeguarding Lead.

5.73 Senior staff and Governors will ensure that the service we receive from Smoothwall has regular checks to ensure that the filtering methods selected are appropriate, effective and reasonable. Smoothwall meets the requirements for an appropriate filter as described by the UK Safer Internet Centre and is used by the majority of schools throughout Cambridgeshire, who are advised by the Cambridgeshire ICT Service.

5.8 Managing videoconferencing

5.81 Where sensitive information is being discussed over video conferencing, Microsoft Teams is preferred to ensure quality of service and security.

5.82 Other videoconferencing software may be used, such as Zoom and SKYPE, but only under close supervision by staff (if pupils are involved) and with permission from the Computing Co-ordinator and/or Child Protection Co-ordinator.

5.83 Pupils must seek permission from the supervising staff member before making or answering a videoconference call.

5.84 The Covid 19 pandemic 2020 has seen all staff utilise teleconferencing technology within school for assemblies enabling all pupils to come together remotely and also between institutions.

Should circumstances arise that video conferencing is necessary in the future, the school would ask parents to agree to behaviour standards and have knowledge of how their child's image is being used (Appendix 4). There is careful consideration of the location that everyone uses. It is possible that children may be in their bedrooms and this may not be appropriate. During live assembly calls parents are contacted instantly if a child's behaviour is inappropriate and the presenter has the power to disable participants' audio and video.

5.85 If a child would need to be contacted by members of staff individually via teleconference. In these instances this is done in school and the Head has knowledge for the reasons and contact is known by parents.

5.9 Managing emerging technologies

Emerging technologies (such as Artificial Intelligence - AI) will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. In February 2024 The children's Commissioner stated, *"Children using AI are potentially exposing themselves to new risks of harm online, and their lives may be reshaped more fundamentally by them in the future. Given its recent emergence, it is unsurprising that the actual impact of AI on children's lives is still not fully understood. Ofcom tracks children's online and media usage, and have found that 59% of 7-17 year old and 79% of 13-17 year old internet users in the UK have used a generative AI tool in the last year. Snapchat's My AI was the most commonly used platform (51%), and there was no difference by gender in the number of children using these tools."*
"….More work is needed to fully understand how children can safely interact with these new technologies, and what strong safeguards should look like."
Children need to be 13 or older to use services such as ChatGPT. As part of our computing curriculum, with guidance from the National Centre for Computing Education, children are taught how to be digitally critical (See 3.1) and identify content that is not real or produced by AI.

5.10 Mobile Phone Use

5.10.1 Mobile phones will not as a matter of course be on display or be used by staff, volunteers or pupils during lessons or formal school time (Please also see section 8.2) Pupils must have written consent from parents to bring a mobile phone to school and it will be securely held by the front desk until the end of the formal school day.

5.10.2 The sending of abusive or inappropriate messages is forbidden, in keeping with the Safer Care of Conduct document.

5.10.3 When offsite, and in agreement with this policy, where contact with pupils or a parent is required the group leader may choose to use their personal phone if appropriate for the situation, likely withholding their number using the 141 prefix.

5.11 Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. (The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). Please also refer to section 4.1r of this policy.

6. Policy Decisions

6.1 Authorising Internet access

6.11 All staff, pupils and governors must read and sign the appropriate 'Acceptable User Policy' (AUP) before using any school ICT resource.

6.12 The school will keep a record of all staff and pupils who sign the AUP

6.13 At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

6.14 Parents will be asked to sign and return a consent form (this forms part of the Pupil AUP).

6.2 Assessing risks

6.21 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 Cambridgeshire County Council (the Local Authority) can accept liability for the material accessed, or any consequences of Internet access.

6.22 The school will audit ICT provision through: formal surveys, frequent formal and informal conversations with pupils and parents about internet use to establish if the online-safety policy is adequate and that its implementation is effective. Where risks are identified intervention will be taken as soon as problems arise. This could be in the form of individual, group or whole class education and involve parents.

6.3 Handling online-safety complaints

6.31 Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the Headteacher. The **Complaints Procedure Policy** will also be followed, with reference to this policy.

6.32 Complaints of a child protection nature must be dealt with in accordance with school child protection procedures (see Safeguarding & Child Protection policy).

6.33 Pupils and parents will be informed of the complaints procedure.

6.34 Discussions will be held with the appropriate Police authority to establish procedures for handling potentially illegal issues.

6.4 Community use of the Internet

Where possible, the school will liaise with local organisations to establish a common approach to online-safety.

7. Communication of Policy and Procedures

7.1 Online-safety rules will be posted around the building and discussed with the pupils at the start of each year and throughout the year. Pupils will be informed that network and Internet use will be monitored.

7.2 All staff will be directed to a copy of this policy and its appendices, and its importance explained. They will be involved with its review.

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

7.4 Parents' attention will be drawn to this policy in newsletters, the school brochure and on the school Web site.

7.5 The Pupil AUP, in addition to being available on the school website as part of this policy, will be published annually in the school newsletter.

8. Use of images

Schools need to be able to balance safeguarding the children and young people in their care and ensuring families are able to experience pleasure and pride at their children's achievements through the use of technology.

The use of images can be divided into four categories:

- Images taken for official school use
- Images taken by parents at school events
- Images taken by the media
- Images taken by third parties

Images taken by school

An image of a child is personal data, consent must be obtained from the parent of a child for any images made such as those used for school web sites, productions or other purposes. It is also important to take into account the wishes of the child, remembering that some children do not wish to have their photograph taken.

A signed consent form should be obtained from the child's parent/carer, and should be kept on the child's file, covering all cases where images of children are to be used.

Parents may withdraw consent at any stage, but they would need to do so in writing.

Images must be maintained securely for authorised school use only, and disposed of either by return to the child, parents, or destroying as appropriate.

Care should be taken in relation to particularly vulnerable children such as those who are in public care, recently adopted or those resettled following on from domestic violence.

Examples:
Photographs of pupils or students are taken for building passes. These images are likely to be stored electronically with other personal data and the terms of the Data Protection Act ***will*** *apply.*

A small group of pupils are photographed during a science lesson and the photo is to be used in the school prospectus. This will be personal data but ***will not*** *breach the DPA Act as long as the children and/or their parents/carers are aware this is happening and the context in which the photo will be used.*

Parents wishing to take images at school events

Increasingly technology is making it easier for images to be misused and it is therefore important that schools take practical steps to ensure that images of children taken by parents and carers and by members of the media, are done so in a way that is in accordance with the protective ethos of the school.

The Data Protection Act does not prevent parents from taking images at school events, but these must be for their own personal use. Any other use would require the consent of the parents of other children in the image.

Examples:
A parent takes a photograph of their child and some friends taking part in the school Sports Day to be put in the family photo album. These images are for personal use and the Data Protection Act does not apply.
Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply. However, if the grandparents published the video on their family website, they must receive permission form the parents of the other children involved.

The head teacher in consultation with governors should agree when parents are to be permitted to take images. This information could be included in invitation letters to parents.
Parents should be required to give an undertaking on how the images will be used. Parents should also be advised that they may only take images in designated circumstances and areas such as in the school hall and not backstage or in changing rooms. It is important that parents understand their responsibilities for the safe keeping of any images they may take.
Consideration should be given to a special photo call session at the end of the event – this would avoid distraction and disturbance and also allow for the withdrawal of children whose parents/carers have not consented.
It is recommended that wherever possible schools take their own 'official' photos or videos in order to retain control over the images produced.
It is also important to ensure that people with no connection with your school do not have any opportunity to produce images covertly. Staff should question anyone who is using a camera or video recorder at events they do not recognise.

Images taken by the press

Example:
A photograph is taken by a local newspaper of a school awards ceremony. As long as the school has agreed to this, and the children and/or their guardians are aware that photographs of those attending the ceremony may appear in the newspaper, this will not breach the Act.

If a child is photographed by a newspaper, the photo becomes the property of the newspaper and the newspaper has the final say as to how it is used. (N.B. images can be placed by editors on the newspaper's website). Generally, newspaper photos of groups of 12+ children do not have the names of the children attached. However, photos of groups of less than 12 children are likely to include the full name of the child in the accompanying caption. Parents need to be aware when they give consent that this is the position. It is important that they are also reminded of the benefits of publicly celebrating achievement to build esteem in the child and pride in their school.

Further advice is available from The Press Complaints Commission who publish a Code of Conduct.

Publishing or displaying photographs or other images of children

The DCSF advise the following,

- If the pupil is named, avoid using the photograph.
- If the photograph is used, avoid naming the pupil.

Whatever the purpose of displaying or publishing images of children care should always be taken to avoid the possibility that people outside the school could identify and then attempt to contact pupils directly. Most abused children are abused by someone they know, but there is still a concern that children might be identified from pictures appearing in the press or other media and targeted for abuse.

Where possible, general shots of classrooms or group activities rather than close up pictures of individual children should be used. The camera angles should be considered. Photographs taken over the shoulder, or from behind are less identifiable.
Children should be in suitable dress, and images of PE or swimming events should maintain modesty, for example wearing team tracksuits if appropriate
Children from different ethnic backgrounds should be included in your communications wherever possible, as well as positive images of children with disabilities to promote the school as an inclusive community, and to comply with the Disability Discrimination Act
Children can be identified by logos or emblems on sweatshirts etc. Depending on the use to which the photograph will be put, airbrushing logos should be considered.
An article could be illustrated by the children's work as an alternative to using an image of the child

It is essential that when considering inviting an official photographer schools establish the validity of the organisation and what checks/vetting has been undertaken. Procedures should also ensure that levels of supervision are appropriate to safeguard the welfare of children at all times when visitors are present on the school site.

There may be occasions where the media take photographs at your school of pupils. It is important that parents and carers are aware of the potential risks and benefits so they can make an informed decision about consent.

Using photographs of children supplied by a third party

Copyright of an image including those downloaded from the internet usually rests with the person who produced it.

Before using an image supplied by a third party, schools should check that the third party owns the copyright of that image and you should obtain their written permission to use it

Schools should ask a third party to guarantee to you that all relevant consents have been given and that they are entitled to provide you with the image.

Websites and Web cams

Consent gained from parents/carers for the use of photographs or videos may not extend to website or web cam use, so it is important to check, when introducing such technology, the status of existing consent for pupils.

It is important to take care with identification, and to respect parental views on the use of any photography of children on a website.

The regulations for using web cams are similar to those for CCTV (closed-circuit television). Children, their parents and other adults appearing on the web cam all need to be consulted and their consent obtained. In gaining consent, you must tell the person why the web cam is there, what you will use the images for, who might want to look at the pictures and what security measures are in place to protect access. In addition the area in which the web cam is being used must be well signposted so that people must know that the web cam is there before they enter the area.

Useful sources of information

The Information Commission website at www.ico.gov.uk
Press Complaints Commission Code of Practice at www.pcc.org.uk/cop/practice.html
Internet Watch Foundation at www.internetwatch.org.uk
Child Exploitation and Online Protection at www.ceop.gov.uk
Teachernet at www.teachernet.gov.uk

8.1 School equipment should be used to take images/video in the vast majority of cases. Personal equipment should only be used in rare instances when there is a legitimate reason for doing so and with express permission of the Head Teacher, given in advance. Memory cards stay in school and images are wiped from memory cards after images are transferred to the school's server.

8.2 There may be occasions in which staff require their mobile phones to be on their person however, staff should not use their personal device whilst working with children unless specifically agreed by the Headteacher in advance. Staff should never use these to take images of children as there is school equipment for this purpose. We follow the guidance as set out in DfE (2024) Mobile Phones in School.

An exception of mobile use for photography is for the updating of Instagram by the Head as this is used to update the front page of the school's website. The majority of images are of children's work. This keeps the website looking current and keeps parents informed of anecdotal incidents that may not make The Star. Images of children may be posted on Instagram but these do not identify the child and where they do, express parental permission has been sought afresh for the individual photo to be posted - both from the child and their parent. The photo is deleted from the mobile device as soon as it is uploaded.

As the capability of mobile devices develop, they can be a useful tool in lessons providing access to voice searches, musical play lists or quick reference to an online dictionary. A personal mobile stays in the adult's possession and should never be given to a child. If a mobile device is paired with a clever touch screen, aeroplane mode should be switched on to prevent notifications. If a child is using an ipad within class, there is an option of using 'guided access', which limits the child to that app.

8.3 Especially in the lower years of a school, images of children undertaking an activity are taken for assessment purposes and stuck into exercise books and on the Seesaw Learning platform. Their Teachers take these books home to mark – this is acceptable as it is a requirement of the job but no copies are to be made and books should be stored securely.

Appendix 1: Pupil Acceptable User Policy & Accompanying Letter to Parents

Dear Parent/ Carer,

Computing, which includes use of the internet, email and mobile technologies, etc. is an important part of learning in our school. It is use in a wide variety of ways to help children learn across all the curriculum areas, as well as providing opportunities to teach specific computing objectives. We expect all children to be safe and responsible when using technology. Online Safety is taught as an integral part of our Computing curriculum and Personal, social, health and economic education.

We encourage children to follow a common set of online-safety rules. Throughout your child's time at Steeple Morden we teach the children:

- How to recognise and to be aware of the risks when online;
- Strategies for protecting themselves against these risks when supported or unsupported by adult supervision, for example that they know to inform a trusted adult (e.g. teacher/parent) immediately if they encounter any material that makes them feel uncomfortable or upset;
- To acknowledge the source of information, when using Internet material for their own use;
- How to think critically about the content they see and the people they interact with online through discussion and mocked-up examples e.g. that the writer of an e-mail or the author of a Web page might not be the person claimed.
- How to validate information before accepting that it is necessarily accurate;
- How to report online concerns bullying or content
- Part of staying safe online includes teaching the children not to share their school account details with anyone, including parents. Other accounts we would expect parents to monitor.

As your child is likely to be very young, please read and discuss the online-safety rules on the reverse of this letter with your child and return the attached slip as soon as possible. If you have any concerns or would like further information or guidance, please contact the school office.

Yours sincerely,

Mr Beavan

Computing Co-ordinator

Pupil Acceptable Use Policy

Agreement & Online-Safety Rules

- ☺ I will only use ICT in school for school related purposes.
- ☺ I will only use my class email address or my own school email address when emailing.
- ☺ I will only open email attachments from people I know, or who my teacher has approved.
- ☺ I will not tell other people passwords, but I will share with my Parent/Carer what I have been doing and who I am interacting with.
- ☺ I will only open/delete my own files.
- ☺ I will make sure that all contact with other children and adults is responsible, polite and sensible, as if we were 'face to face'. As the internet is a public place, I will not do anything online which I would not be happy to appear on the front of a newspaper.
- ☺ I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell an adult immediately.
- ☺ I will not give out my own personal details such as my name, phone number or home address.
- ☺ When in Year 2 or above we will use Google Classroom and a program called Mathletics to help improve our maths skills, my parent/carer agrees to allowing my name, year group and activity scores to be held securely by 3plearning, who are the people who run the Mathletics website, to allow me to access the activities with a user name and password especially for me
- ☺ I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- ☺ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- ☺ I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or have the potential to embarrass myself or any member of the school community.
- ☺ I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my online-safety.

Pupil Acceptable User Policy

We have discussed this and agree to follow the Online-Safety rules and to support the safe use of ICT at Steeple Morden Primary School.

Parent/ Carer Signature ……

Child/ren.....

I/We agree to follow the online-safety rules to stay safe and be kind to others.

Class(es) …… Date ……

Appendix 2: Staff and Governor Acceptable User Policy

Staff & Governor ICT Agreement & Acceptable Use Policy

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Online-Safety Coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies (including staff laptops) for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal email address, without authorisation from the Headteacher.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Headteacher or Governing Body.
- I will not install any hardware of software without permission of the ICT Coordinator or Headteacher.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and staff will only be taken, stored and used for professional purposes in-line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/carer, member of staff and Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's Online-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

Staff & Governor ICT Agreement & Acceptable Use Policy

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school.

Signature _____ Date _____

Full Name _____ (printed)

Job title

(if appropriate) _____

Appendix 3: Internet use - Possible teaching and learning activities

Activities	Key online-safety issues	Relevant websites
Creating web directories to provide easy access to suitable websites.	Parental consent (sought through the General Consents Form). Pupils should be supervised. Pupils should be directed to specific, approved on-line materials.	Web directories e.g. Ikeep bookmarks Webquest UK Kent Grid for Learning (Tunbridge Wells Network)
Using search engines to access information from a range of websites.	Parental consent (as above). 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.	CBBC Search Google
Exchanging information with other pupils and asking questions of experts via e-mail.	Pupils should only use approved e-mail accounts. Pupils should never give out personal information. Consider using systems that provide online moderation.	E-mail a children's author E-mail Museums and Galleries
Publishing pupils' work on school and other websites.	Pupil and parental consent should be sought prior to publication (as above). Pupils' full names and other personal information should be omitted.	Making the News SuperClubs Infomapper Headline History Kent Grid for Learning Focus on Film
Publishing images including photographs of pupils.	Parental consent for publication of photographs should be sought (as above). File names should not refer to the pupil by name.	Making the News SuperClubs Learninggrids Museum sites, etc. Digital Storytelling BBC – Primary Art
Communicating ideas within chat rooms or online forums.	Only chat rooms dedicated to educational use and that are moderated should be used. Access to other social networking sites should be blocked. Pupils should never give out personal information.	
Audio and video conferencing to gather information and share pupils' work.	Pupils should be supervised. Only sites that are secure and need to be accessed using an e-mail address or protected password should be used.	Skype National Archives "On-Line" National History Museum Imperial War Museum

Approved by the Governing Body:	December 2024
This policy is to be reviewed:	Annually
The next review date is:	December 2025
Review is the responsibility of:	Curriculum Committee

Signed:  Dated: 10th December 2024

Headteacher