E-Safety & Appropriate Use of ICT Policy

Steeple Claydon Primary School and

Pre-School

Approved by: Governor Resources Committee	Feb 23	**Date:** Spring 2023
Last reviewed on:	Spring 2023	
Next review due by:	Spring 2026	

Contents

1 Introduction

2 Roles and Responsibilities

3 E-Safety in the Curriculum

4 Children with Additional Needs

5 E-Mail

6 E-Safety Support for Staff

7 The Internet

8 The Taking of Images and Film

9 Publishing Children' Images and Work

10 Storage of Images

11 Web Cams and CCTV

12 Video Conferencing

13 Personal Mobile Devices

14 Learning Platform

15 Cyber-Bullying

16 Parental Involvement

17 Security

18 Breaches

19 Incident Reporting

20 Protecting Personal, Sensitive, Confidential Information

21 Viruses

22 Disposal of ICT Equipment

23 Zombie Accounts

Appendices

1 Acceptable Use Agreement for Staff

2 Acceptable Use Agreement for Children and Parents

What is e-safety?

E-safety covers issues relating to children as well as adults and their safe use of the internet, mobile devices and other electronic communication devices. It includes education for all members of the school community on risks and responsibilities and is part of the school's 'duty of care'.

Our school E-Safety Policy has been written by the school, building on government and local authority guidance and other local school's e-safety policies.

The E-Safety Policy relates to other policies including those for ICT, bullying, child protection and safeguarding.

1 Introduction

ICT 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.

Information and Communications Technology (ICT) 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 ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites/internet
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, 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 and that some have minimum age requirements, usually 13 years.

At Steeple Claydon School, we understand the responsibility to educate our children on E-Safety issues; teaching them the appropriate behaviours to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

2 Roles and Responsibilities

E-Safety is an important aspect of the strategic leadership within the school. The Head teacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The Head teacher is the E-Safety Co-ordinator, who has been designated this role as a member of the senior leadership team. All members of the school community are aware of who holds this post. This role may also be covered by a Designated Safeguarding Lead as the roles overlap. It is not a technical role.

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and children, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: Child Protection, Health and Safety, Behaviour (including anti-bullying) and PSHE.

3 E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the children on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- The school provides opportunities to teach children about E-Safety
- Children are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Children are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cyber Mentors, Childline or CEOP report abuse button.
- Children are taught to critically evaluate materials and learn good and safe searching skills

4 Children with Additional Needs

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

people.

5 E-Mail

The use of e-mail within school is an essential means of communication. In the context of school, e-mail should not be considered private. We recognise that children need to understand how to style an e-mail in relation to their age and good network etiquette or 'netiquette'.

- All e-mails written should be checked carefully before sending, in the same way as a letter written on school headed paper. For adults, work emails to outside agencies and parents should be sent via the school email address.

- Children may only use school approved accounts on the school system and only under direct teacher/parent supervision for educational purposes.

- E-mails created or received as part of the school job are subject to disclosure in response to a request for information under the Freedom of Information Act 2000.
- Sensitive and/or pupil information should only be sent via school email system.

- The forwarding of chain letters is not permitted in school.

- All child e-mail users are expected to adhere to the generally accepted rules of 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, virus checking attachments. E-mails must not be used by any member of the school community to send or receive indecent or offensive images, videos or any written material of this kind. In addition, e-mails must not be used by any member of the school community to cause intentional harm, upset, directly or indirectly to others.

- Children must immediately tell a teacher/trusted adult if they receive an offensive e-mail whether directed at themselves or others and before it is deleted.

- Staff must inform the Headteacher if they receive an offensive e-mail whether it is directed at themselves or others and before it is deleted.

- Children are introduced to e-mail as part of the ICT Scheme of Work.

- When school e-mail is accessed, (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

Sending E-Mails

- Staff are to keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

- Staff should not send or forward attachments unnecessarily. Whenever possible, they should send the location path to the shared drive rather than sending attachments.

- School e-mail is not to be used for personal advertising.

Receiving E-Mails

- Check e-mails daily using approved school email system.
- Never open emails or attachments from an untrusted source; consult the office or technician first if in doubt.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of e-mails is not allowed.

6 E-Safety Support for Staff

Our staff receive annual and appropriate information and training on E-Safety and how they can promote the 'Stay Safe' online messages. This is usually through the usual scheduled programme of staff meetings.

New staff receive information on the school's acceptable use policy as part of their induction.

All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of E-Safety and know what to do in the event of misuse of technology by any member of the school community.

All staff incorporate E -Safety activities and awareness within their curriculum areas.

7 The Internet

The internet is an open worldwide communication medium, available to everyone, 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 internet is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school provides children with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with children.
- 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. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.
- On-line gambling or gaming is not allowed.

- All staff, parents/carers, volunteers and governors must comply with the Code of Conduct regarding the posting of any information or images relating to the school.

- School internet access is controlled through a web filtering service provided by Turn IT On.

- Steeple Claydon School is aware of its responsibility when monitoring staff communication under current legislation.

- Staff and children are aware that school-based e-mail and internet activity can be monitored and explored further if required.

- The school does not allow children access to internet logs.

- If staff or children discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the E-safety Co-ordinator or teacher as appropriate.

- It is the responsibility of the school to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

- Children and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Headteacher

- If there are any issues related to viruses or anti-virus software, the Headteacher should be informed.

- The school does not allow any access to social networking sites other than those approved for educational purposes i.e. a virtual learning environment (VLE)

- Staff or pupil personal information will not be published on the school website. Any contact details on line should be the school office.

- After permission has been obtained from parents or carers, pupil photographs/work may be published on the school website. Pupil image file names will not refer to the pupil by name.

- With regard to the school's website, the Headteacher takes overall editorial responsibility and ensures that content is accurate and appropriate.

We believe that it is essential for parents/carers to be fully involved with promoting e- safety both in and outside of school and to be aware of their responsibilities. We annually consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

8 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 children) and staff, the school permits the appropriate taking of images by staff and children with school equipment

- Staff, parents/carers and visitors are not permitted to use **personal** digital equipment, such as mobile phones and cameras, to record images of children; this includes when on field trips, unless there is prior agreement from the head teacher. Appropriate images can be taken using school cameras; these should be transferred as soon as possible to the school's network and deleted

from the individual device.

- Children are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of children, staff and others without advance permission from the Headteacher.

- Staff must have permission from the Headteacher before any image can be uploaded for publication.

- Where an outside company or individual is commissioned by the school to take images, there must be appropriate DBS clearance and the school should satisfy itself that appropriate arrangements are in place to ensure images are not stored or distributed outside of the school.

9 Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site.

- in the school handbook and other printed publications that the school may produce for promotional purposes.

- recorded/ transmitted on a video or webcam.

- in display material that may be used in the school's communal areas.

- 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)

- On school social media such as Facebook

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 or carers may withdraw permission, in writing, at any time.

Children' names will not be published alongside their image and vice versa. E-mail and postal addresses of children will not be published. Children' full names will not be published. Before posting a child's work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

10 Storage of Images

- Images/ films of children are stored on the school's network.

- Children and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks).

- Rights of access to this material are restricted to the teaching staff and children within the confines of the school network or other online school resource.

11 Web Cams

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes and our children's use of webcam is appropriately supervised for the pupil's age.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document). Where possible, webcams should be turned off when not in use.

12 Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- All children are supervised by a member of staff when video conferencing.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- No part of any video conference is recorded in any medium without the written consent of those taking part.
- Video conferencing should use the educational broadband network to ensure quality of service and security.

13 Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- All mobile phones must be turned off or on silent and kept in a cupboard in the classroom or in the staff room, away from the children. They must not be used while working with children unless specific permission has been given by the headteacher, for example to receive an urgent telephone call.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate messages, images (including pseudo images), videos or sounds between any members of the school community (staff, parents/carers, pupils) is not allowed.
- The creation of inappropriate messages, images (including pseudo images), videos or sounds by any member of the school community is not allowed.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Children's mobile phones and/or personal devices are to be handed to their teacher and are not permitted for use during the school day.

14 Learning Platforms

The staff will regularly monitor the usage of any Virtual Learning Platform (VLE) by children and staff, in particular monitoring messaging and communication tools.

Children and staff are advised about acceptable conduct and use when using the VLE and how to report any concerns of misuse

Only members of the current school community have access to the VLE.

15 Cyber-bullying

Cyber-bullying is defined as, 'The use of ICT, particularly mobile phones and the internet, to deliberately hurt or upset someone.' DCSF 2007

Cyber-bullying (along with other forms of bullying) of any member of the school community will not be tolerated.

All incidents of cyber-bullying whilst using school facilities will be investigated and recorded, in line with the school's Anti-bullying Policy.

16 Parental Involvement

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.

  Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website or sharing platform such as Seesaw).

17 Security

The school gives relevant staff access to its Management Information System, with a unique username and password

- It is the responsibility of everyone to keep passwords secure; passwords are not to be shared with others
- Staff are aware of their responsibility when accessing school data
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use
- Staff keeps all school related data secure. This includes all personal, sensitive, confidential or classified data
- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under control at all times
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

- All ICT equipment is security marked as soon as possible after it is received. The Office Administrator maintains a register of all ICT equipment and other portable assets.

- As users of the school ICT equipment, staff are responsible for their activity.

- ICT equipment issued to staff is logged and serial numbers are recorded as part of the school's asset register.

- It is imperative that staff save data on a frequent basis to the school's network. Staff are responsible for the backup and restoration of any data that is not held on the school's network.

- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.

- Privately owned ICT equipment should not be used on a school network.

- On termination of employment, resignation or transfer, staff must return all ICT equipment to the school. Staff must also provide details of all their system log-ons so that they can be disabled.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting a journey.

- The installation of any applications or software packages must be authorised by the ICT Subject Leader or the Headteacher.

- Portable equipment must be transported in its protective bag.

Server Security

- School servers are kept in a locked and secure environment and there are limited access rights to these which are password protected.

- Existing servers have security software installed appropriate to the machine's specification and the school uses a remote back up service with data being backed up daily.

Using Removable Media

- Always consider if an alternative solution already exists.
- Only use recommended removable media.
- Store all removable media securely.
- Removable media must be disposed of securely by your ICT support team.

Monitoring

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

mobile phones and other mobile devices.

- Internet activity is logged by the school's internet provider and in addition the school's technicians regularly monitor the web sites which are accessed on school equipment.

18 Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school policy, breaches may also lead to criminal or civil proceedings.

19 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's E-Safety Co-ordinator and/or Head teacher. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Headteacher.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Headteacher, depending on the seriousness of the offence; investigation by the Headteacher/ LA, possibly leading to disciplinary action, dismissal and involvement of police for very serious offences.

- Complaints/concerns of a child protection nature must be dealt with in accordance to the school's child protection procedures.

20 Protecting Personal, Sensitive, Confidential and Classified Information

Staff will ensure:

- They lock their screen before moving away from their computer during the normal working day to prevent unauthorised access

- Personal, sensitive, confidential or classified information is not disclosed to any unauthorised person

- The security of any personal, sensitive, confidential and classified information contained in documents which are faxed, copied, scanned or printed is not compromised

- They only download personal data from systems if expressly authorised to do so by the Headteacher

- They keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information

- Hard copies of data are securely stored and disposed of after use in accordance with the document labeling

- They protect school information and data at all times, including any printed material

21 Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Staff must never interfere with any anti-virus software installed on school ICT equipment that you use.

- If any machines are not routinely connected to the school network, staff must make provision for regular virus updates through the IT team.

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

22 Disposal of ICT Equipment

- All redundant ICT equipment will be disposed of through an authorised agency recommended by the LA. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate and if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.

Disposal of any ICT equipment will conform to current legislation and will confirm with the governors' policy on the disposal of equipment.

23 Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

Technical staff will ensure that all user accounts are disabled once the member of the school has left the school.

Appendix 1

Steeple Claydon School - E-safety policy

Acceptable/Responsible Use Agreement for Staff

- I will only use the school's email, internet, network and any related technologies for professional purposes or for uses defined as 'reasonable' by the Headteachers or governing body.

- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately on school premises. Personal data can only be taken out of school when authorised by the Headteacher.

- I will not install any hardware or software without permission of the Headteacher or ICT Subject Leader.

- I am aware that I may use my school laptop for personal use, however I must ensure that at no time this is being used inappropriately or inappropriate material is being accesses – this includes any materials that could be considered offensive, illegal or discriminatory. I will ensure that my use of ICT is in keeping with the E Safety Policy.

- I am aware that ICT technical staff monitor the use of ICT and the internet and that if I am found to have accessing inappropriate material or using ICT inappropriately this may result in disciplinary action being taken.

- If I have any concerns about any incidents where inappropriate pop-ups or other material inadvertently appears I must log this immediately in the ICT incident log and report this to the Headteacher.

- 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 children and staff are compatible with my professional role.

- I will not give out personal details such as mobile phone numbers and personal email addresses to children.

- I will support and promote the school's E-Safety Policy and data security and help children to be safe and responsible in their use of ICT and related technologies.

- I will ensure that photographs of children (or staff) will only be taken with school equipment and where the parents' permission has been obtained.

- I will ensure that images of children are not stored on any personal equipment or devices.

- I will ensure that I am complying with the Policy on Social Networking Sites and Personal Internet Presence for School Staff and that at no time any images or materials are distributed outside the school without the express permission of the Headteacher.

Signed: _____ Date: _____

Print name: _____

Appendix 2

Children's Agreement:
E-SAFETY RULES

All children wishing to access the internet on site are required to read and sign this document as a record of their acceptance and understanding of our internet safety rules.

As a pupil at Steeple Claydon School, I will…

- Only use age appropriate websites and games and not give out any personal details to anyone.
- Understand that the information I need to keep private includes my full name, address, phone number, name of school and my email address.
- If I come across something upsetting, illegal or scary while I'm online, I will tell a member of staff.
- I know I should minimise my screen and put my hand up immediately if I see something I do not like online.
- I will follow the rules agreed with my class teacher using online resources at all times when going online at school.
- I will treat all of our school equipment with respect and handle it carefully, always returning it back to its correct place when I have finished with it.

Child:

- I understand that these rules are in place for my own safety and the safety of everyone in school.
- I know that if I break these rules, I may not be allowed to access the internet at school.

Signed: _____ Date:_____

Name (printed): _____ Class: _____

Inappropriate use of Social Media:

Nationally social media websites are being increasingly used to fuel complaints and campaigns against schools, school staff, Head Teachers and in some cases parents and children. Steeple Claydon School considers the use of social media in this way as unacceptable and not in the best interests of the children or the school community. Any concerns parents may have should be addressed using the appropriate channels by speaking initially to the class teacher, then the Head Teacher, or eventually to the Chair of Governors, so that they can be dealt with fairly, appropriately and effectively for all concerned.
In the event that any child, or parent of a child being educated at our school, is found to be posting libellous or defamatory comments on Facebook or other social media sites which are personal or would bring the school into disrepute, they will be reported to the 'report abuse' section of the network site. All social media networks have clear rules about the content that can be posted and provide robust mechanisms to report activity which breaches these. The school will also expect that the child or parent removes such comments immediately.

Should any member of the school community use ***any*** social media site to publicly humiliate another this will be taken very seriously, and will be treated as an incidence of bullying behaviour which is not tolerated in our school.

In serious cases the school will consider its legal options to deal with any mis-use of social networking sites.

Parent/Carer:

- I have read and discussed the rules with my child and confirm that he/she has understood what they mean.
- I understand that if my child breaks these rules, they may not be allowed to access the internet using school equipment.
- I understand that filtered internet access will be provided on all of the devices at Steeple Claydon School and that children will be supervised whilst accessing the internet.
- I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I have read, understood and will follow the above paragraph about inappropriate use of social media.

Parent/Carer Signature: _____

Name (printed): _____