We are kind – We show respect – We work hard – We are honest

E-Safety Policy

Date: October 2025

Review date: October 2026

E SAFETY POLICY

Introduction

- E-Safety encompasses Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- This policy was reviewed in September 2025 to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole and incorporates the previous Internet Policy and Staff Acceptable Use Policy. It was also updated to reflect the recent changes to the KCSIE document 2025.
- The school has a duty to provide pupils with access to quality learning using internet technologies and electronic communications and, with this, the responsibility to ensure that this learning takes place safely.
- This e-Safety Policy is an important and integral part of the school's safeguarding procedures.
- Our e-Safety Policy has been agreed by senior leaders and approved by governors.

Associated Policies:-

The school's e-safety policy operates in conjunction with other policies including: Safeguarding & Child Protection; Computing; Behaviour and Anti-Bullying.

Co-ordination of e-Safety

The school has designated two members of staff to lead on e-Safety. They are:

- Mr Connor Worrall, Computing Coordinator
- Mr Fennell, Headteacher and Designated Safeguarding Lead

Contents:

1. Guidelines & Policy Statement for the use of Internet technologies and electronic communications

- All members of staff, including supply teachers and support staff, must have read through this policy statement before a system login password is granted and ICT resources are used.
- All children must be made aware through class discussion of all the important issues relating to acceptable use, especially the monitoring of Internet use. Please refer to the Computing scheme of work for e-safety.
- Internet access is possible for staff and children throughout their hours in school, and so these guidelines are always in operation.
- Access will be specifically designed for pupil use and will include age-appropriate filtering.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.
- Pupils will be shown how to publish and present information to a wider audience.
- Pupils will be taught how to evaluate Internet content.
- Pupils will be taught the importance of cross-checking information before accepting its accuracy – particularly with the growing use of AI.
- Pupils will be taught how to report unpleasant Internet content to staff.
- Children will be taught about the risk of Online Bullying, how to avoid it and what to do if it happens, during lessons on Internet Safety.
- Staff will always use a child-friendly safe search engine when accessing the web with pupils.
- Children must not be given unsupervised access to the Internet. For the purposes of this policy, "supervised" means that the user is under the direct responsibility of an adult.

- The teaching of Internet safety is included in the school's Computing Scheme of Work, but all teachers within all year groups should be including Internet safety issues as part of their discussions on the responsible use of the school's computer systems.
- Pupils need to understand that any unacceptable comments made online can be traced and that this will be viewed as a behaviour issue.
- While the school network is protected by strict filtering systems, in the unlikely event that inappropriate material is encountered, pupils will be taught to lower or switch off their screen and report it to a member of staff immediately.
- Pupils are expected to observe the rules of responsible internet use and are informed that checks can and will be made on files held on the system and the sites they access.
- Pupils will be educated to take responsibility for their own Internet access.

2. Managing Internet Access

a. Social networking, email & messaging systems

- The school's filtering will block access to social networking sites from school.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary-aged pupils, and only moderated social networking sites should be used for this age range. Parents will be informed that the minimum age for accessing most well-known sites is 13 (Y8).
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will be advised to use nicknames and avatars when online
- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail
- In e-mail communication, pupils must not reveal their personal details or those of others or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious, and attachments should not be opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- Instant messaging systems are not permitted on the school's IT systems. Advice will be given to pupils as to how to manage these at home.

b. Managing Internet Publishing

The school wishes the school's website reflects the diversity of activities, individuals and education that can be found at Standhill Infants' School. However, the school recognises the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication on the Internet, the following principles must be followed:

- Pupils' full names will not be used anywhere on a school website or other online space, particularly in association with photographs or video material. Surnames must never be published
- No link should be made between an individual and any home address (including simply street names).
- Where the person publishing material suspects that there may be child protection issues at stake, then serious consideration must be taken as to whether that material may be published or not. In the case of a

simple piece of artwork or writing, this may well be fine, but images of that child should not be published. If in any doubt at all, refer to the person responsible for child protection.

- Staff or pupil personal contact information will not be published. The contact details given online should be for the school office or class email accounts.
- The persons responsible for eSafety have overall editorial responsibility and will work to ensure that content is accurate, appropriate and does not breach eSafety guidelines
- However, all staff have individual responsibility to ensure that these eSafety guidelines are adhered to and must be proactive in implementing them
- When publishing pupils' images and work, photographs that include pupils should be selected carefully so that individual pupils cannot be identified or their image misused. Using group photographs rather than full-face photos of individual children is the preferred option
- Permission from parents or carers will be obtained before photographs of pupils are published on the school website. This will normally be through the permission form sent out to all pupils on entry. Separate permission will be sought for use by third parties.
- Pupil image file names will not refer to the pupil by name.
- Parents should be made aware of the school's rules about taking and sharing photos, whether on school websites or other online platforms.

c. Managing videoconferencing & webcam use

- Videoconferencing should use the educational broadband network to ensure quality of service and security.
- Videoconferencing and webcam use will be appropriately supervised for the pupils' age.

d. Managing emerging technologies

- Emerging technologies will be examined for educational benefit, and a risk assessment will be carried out before use in school is allowed.
- The eSafety coordinators are aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications and will develop further guidelines as necessary.
- Mobile phones are not allowed to be used in school and will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden.
- The use of mobile phones for taking photographs is not permitted at school.

e. Security

- Access is limited to the use of authorised accounts and passwords, which should not be made available to any other person.
- The school will work with ATOM ICT services to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator or Headteacher.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Filtering of the network will be set at the level approved by the LA.s

- No changes to the level of filtering will be allowed without a Risk Assessment and the permission of the Headteacher
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- School ICT systems security will be reviewed regularly.
- Virus protection is updated regularly using the Local Authority-approved system and technical support.
- Security strategies are discussed with the Local Authority through regular contact with the IT support service.

f. Monitoring & Actions to Maintain eSafety

- All staff must be proactive in their monitoring of children using internet technologies
- The ICT coordinator will regularly monitor system use.
- If there is an incident in which a pupil is exposed to offensive or upsetting material the school will respond to the situation quickly and on several levels. Responsibility for handling incidents is taken by the eSafety Coordinators (Headteacher and Computing Coordinator) and the Designated Child Protection Officer, if necessary, and the pupil's class teacher. All teaching staff will be made aware of the incident at a Staff Meeting if appropriate.
- If one or more pupils discover (view) inappropriate material our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue.
- If staff or pupils discover unsuitable sites, the Computing coordinator/eSafety coordinator will be informed and will report the URL (address) and content to the LA Helpline and ATOM IT. This may be referred further to CEOP, Internet Watch Foundation, or the police.
- It is the duty of all staff to report any transgressions of the school's Internet policy to the eSafety Coordinator.
- Serious 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.
- Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.
- Referrals to other agencies, including the Police, will be made for potentially illegal issues.
- The Headteacher or Deputy Headteacher will deal with any issues of Online Bullying in accordance with the school's anti-bullying.
- It is for the Headteacher to decide upon the appropriate course of action or sanction. Transgressions of Internet Policy and use of inappropriate language can be dealt with in a range of ways, including removal of Internet access rights; computer system access rights; meetings with parents or even exclusion, in accordance with the severity of the offence and the school's Behaviour Policy.
- Pupils and parents will be informed of the consequences for pupils misusing the Internet.
- All serious transgressions of the school's eSafety Policy are recorded on CPOMS.
- Breaches of Internet Access Policy by staff will be reported to the Headteacher and will be dealt with according to the school's and LA's disciplinary policy, or through prosecution by law.
- Within the E-Safety Curriculum, children are taught about the safe and appropriate use of AI. This will ensure that pupils benefit from a knowledge-rich curriculum that enables them to become well-informed users of technology and understand its impact on society. Children are taught how to protect themselves against harmful or misleading content.

g. Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Nottinghamshire County Council can accept liability for any material accessed, or any consequences of Internet access.
- The school constantly monitors the use of IT to establish if the e-safety policy is adequate, that the implementation of the e-safety policy is appropriate and effective and if any improvements are needed.
- Online challenges, hoaxes, misinformation, disinformation, conspiracy theories, and emerging risks such as the misuse of AI can pose significant threats to children's wellbeing and understanding of the digital world. These issues can spread quickly across social media and online communities, encouraging unsafe behaviour, promoting false or misleading narratives, and manipulating young people's perceptions of reality. As part of our school's commitment to online safety, we aim to equip the children with the critical thinking skills needed to evaluate digital content, recognize deceptive or harmful information, and understand how AI-generated material can be used responsibly—or misused to mislead others. Through education, supervision, and clear reporting pathways, we strive to create a safe and informed online environment where children can navigate digital spaces with confidence and caution.

h. Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school website.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

3. Staff Acceptable Use Policy and eSafety Guidelines

- Professional use of the computer system is characterised by activities that provide children with appropriate learning experiences or allow adults to enhance their own professional development.
- All staff, with access to the school's IT network, will be given the school e-Safety Policy and its importance in ensuring child safety.
- Staff must understand that network and Internet traffic can be monitored and traced to the individual user.
- Staff must ensure that the copyright of materials is respected. When using downloaded materials, including free materials, the Intellectual Property rights of the originator must be respected and credited. Staff will be briefed about the use of Creative Commons images and pass this on to pupils. All material saved on the school's network is the property of the school and making unauthorised copies of materials contained thereon may be in breach of the Data Protection Act, Individual Copyright or Intellectual Property Rights.
- Posting anonymous messages and forwarding chain letters is prohibited.
- The use of the Internet, e-mail, or any other media to access inappropriate materials such as pornography, racist or any other offensive material is forbidden.
- All web activity is monitored, including the content of e-mail, therefore, it is the responsibility of the user to ensure that they have logged off the system when they have completed their task.
- Activity that threatens the integrity of the school's computer systems, or that attacks or corrupts other systems, is prohibited.

- Users are responsible for the content of all e-mail sent and for contacts made that may result in e-mail being received. Due regard should be paid to the content of emails, whether or not this is sent from a school email address. The same professional levels of language should be applied as for letters and other media.
- Use of the school's Internet for personal financial gain (including the use of online auction sites), gambling, political purposes or advertising is excluded.

a. Staff Guidance on the use of Social Networking and messaging systems

- The school recognises that many staff will actively use Facebook, Twitter and other such social networking, blogging and messaging services. It is recognised that some such services may have an appropriate application in school, however, where such activities are planned a separate account should be set up for the purpose and there should be no connection made between personal and school accounts used for educational purposes. Any such accounts and activities should be approved by a member of the SLT prior to use.

- Although these networks are used by staff in their own time, staff must recognise that it is not appropriate to discuss issues relating to children or other staff via these networks. Staff are encouraged to review their privacy settings to make sure that their profiles and photographs are not viewable by the public.

- It is never acceptable to accept a friendship request from a child from school, as in almost all cases, children of primary age using such networks will be breaching the terms and conditions of use of those networks. It is also extremely inadvisable to accept as friends ex-pupils who are still minors.

- Staff are required to follow these guidelines and always demonstrate acceptable conduct when using the school's IT systems and act professionally when accessing the internet from home. The school's and Local Authority Disciplinary Procedures will be used in case of misuse or unprofessional conduct.

b. Use of ICT Equipment

The computer system is owned by the school. "The computer system" means all computers and associated equipment belonging to the school, whether part of the school's integrated network or stand-alone, or taken off-site. The school provides portable ICT equipment such as laptop computers, iPads, voice recorders, video cameras and digital cameras to enhance the children's education and to allow staff to make efficient use of such equipment to enhance their own professional activities.

- The installation of software or hardware unauthorised by the school, whether legitimately licensed or not, should be checked with either the ICT coordinator or Headteacher before proceeding.

- The school reserves the right to examine or delete any files that may be held on its computer systems and to monitor any Internet sites visited.

- All personal data held on the school's network is subject to the Data Protection Act 1998 and the school's Data Protection Policy.

- Equipment may be in the care of a specific individual, but it is expected that all staff may wish to benefit from the use of a laptop computer and access should be negotiated with the individual concerned. Any difficulties should be referred to the ICT co-ordinator.

- Certain equipment will remain in the care of the ICT co-ordinator and may be used according to staff requirements. Once equipment has been used, it should be returned to the resource area.

- Equipment such as laptop computers is encouraged to be taken offsite for use by staff in accordance with this Acceptable Use Statement and Internet Access guidelines and that the equipment is fully insured from the moment it leaves the school premises.

- Any costs generated by the user at home, such as phone bills, internet connection, printer cartridges etc., are the responsibility of the user.

- Where a member of staff is likely to be away from school through illness, professional development (such as secondment etc), or maternity leave, arrangements must be made for any portable equipment in their care to be returned to school. In the event of illness, it is up to the school to collect the equipment if the individual is unable to return it.

- If an individual leaves the employment of the school, any equipment must be returned.

- Care should be taken over the use of USB devices to transfer data from external computer systems. Where information has been downloaded from the internet or copied from another computer, wherever possible, it should be emailed to the school to ensure that it undergoes anti-virus scanning.

- Staff may install software on laptops to connect to the Internet from home. Advice needs to be taken before attempting this.

- No other software, whether licensed or not, may be installed on laptops in the care of teachers as the school does not own or control the licences for such software.

- Where data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. It must not be transferred to home computers and should be removed from any portable device, including USB devices and memory cards as soon as is practical. Where staff are using their own digital equipment, such as cameras and mobile phones, extreme caution is advised to avoid misinterpretation by others. Files should be transferred to the school equipment as soon as possible.

- Wherever practical, use of portable media (USB sticks/Portable Hard-Drives) must be avoided for the transporting of important and/or sensitive data. Original work most not be saved solely on a portable media device. If sensitive data has to be transferred by such portable media, its security should be considered carefully.

- Staff should utilise 'Microsoft One Drive' as the main file hosting service to ensure the security of important and/or sensitive data is maintained and used is to be used as the main alternative to USB sticks.

The e-Safety Policy was revised by: C Worrall

Date: October 2025

Review: October 2026

APPENDIX 1
Staff Acceptable Use Agreement

The following guidelines have been drawn up to ensure that staff are fully aware of their responsibilities with respect to their use of school ICT equipment, both at home and school, and are asked to sign this acceptable use agreement.

- The computer networks is the property of the school, and I agree that my use must be compatible with my professional role.
- The school ICT systems may not be used for private purposes without specific permission from the headteacher.
- Use for personal financial gain, gambling, political purposes, advertising or to access inappropriate materials is forbidden.
- I agree that the school may monitor my network and Internet use to ensure policy compliance.
- I will respect ICT system security and understand that it is a criminal offence to use a computer for a purpose not permitted by its owner.
- Software or hardware must not be installed without permission.
- My password and login name to the network are confidential and should not be shared with pupils
- All reasonable precautions to secure data or equipment taken off the school premises must be made, e.g., remove laptops from vehicles, keep them secure at home.
- I will report any incidents of concern to the school Designated Child Protection Coordinator or e-Safety Coordinator as appropriate.
- I will ensure that my electronic communications with pupils are compatible with my professional role and cannot be misinterpreted.
- I will promote e-safety with the pupils that I work with and will help them to develop a responsible attitude to ICT use.
- I will respect copyright and intellectual property rights.
- I will report to the appropriate person any possible security threats, inappropriate materials, etc., on my laptop before reconnecting to the school network
- I have received and read a copy of the school's eSafety Policy, including the Staff Acceptable Use section and agree to follow its guidelines

The school will exercise its right to examine the use of the school's computer systems, including access to websites, the interception of e-mail and the deletion of inappropriate materials, where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes.

Signed: …….. Capitals: ……

Accepted for School: …….. Capitals: ……..

Date: ……..

APPENDIX 2

Carlton Standhill Infants' School Pupil Internet Agreement

When you've read this with your parent(s) and signed it, please bring it back to school.

- ❑ I will be responsible for my own behaviour on the Internet, just as anywhere else in school.
- ❑ If I see something I am unhappy with or receive a message I do not like, I will tell a member of staff immediately to protect myself and other pupils.
- ❑ **I** will not try to find websites in school that are not to do with my work or which I know will be offensive, rude or unpleasant.
- ❑ I understand that the school may monitor the Internet sites I visit.
- ❑ I will not take part in any bullying using phones, messaging or other IT equipment and will tell someone if I know someone else in school is.
- ❑ I will not use any rude language when commenting on the website, in emails and on my learning space.
- ❑ I will only use the internet with permission from a member of staff.
- ❑ I will not access other people's files unless permission has been given.
- ❑ I will only use computers for schoolwork and homework unless permission has been granted otherwise.
- ❑ I will not download any programs to the computer from the Internet and I will not bring programs from home for use in school.
- ❑ I will not print on our network unless I have asked for permission.
- ❑ I will not give out personal information such as full name, phone number and address and will tell an adult if anyone tries to make arrangements to meet me.
- ❑ I will only use e-mail accounts provided by the school and will not try to use instant messaging in school.
- ❑ If I choose not to follow these rules, I understand I will not be allowed access to Internet resources and be in trouble for poor behaviour.

I have read through this agreement with my child and agree to these safety restrictions.

Signed: _____ (Parent/Responsible Adult)

Name of child: _____

Appendix 3:

Useful resources for parents

- What are the issues? UK Safer Internet Centre: https://saferinternet.org.uk/guide-and-resource/what-are-the-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
- Internet Matters – Pre-school resources. https://www.childnet.com/

Online safety advice

Childnet – Provides guidance for schools on cyberbullying

Educateagainsthate – Provides practical advice and support on protecting children from extremism and radicalisation

London Grid for Learning – Provides advice on all aspects of a school or college's online safety arrangements

NSPCC E-safety for schools – Provides advice, templates, and tools on all aspects of a school or college's online safety arrangements

Safer recruitment consortium – 'Guidance for safe working practice', which may help ensure staff behaviour policies are robust and effective

Searching screening and confiscation – Departmental advice for schools on searching children and confiscating items such as mobile phones

South West Grid for Learning – Provides advice on all aspects of a school or college's online safety arrangements

Use of social media for online radicalisation – A briefing note for schools on how social media is used to encourage travel to Syria and Iraq

Online Safety Audit Tool – From UK Council for Internet Safety to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring

Online safety guidance if you own or manage an online platform – DCMS advice

A business guide for protecting children on your online platform – DCMS advice

UK Safer Internet Centre – Provides tips, advice, guides and other resources to help keep children safe online

Online safety relating to remote education, virtual lessons and live streaming

Guidance Get help with remote education – Resources and support for teachers an

school leaders on educating pupils and children

Departmental guidance on safeguarding and remote education – Including planning remote education strategies and teaching remotely

London Grid for Learning – Guidance, including platform-specific advice

National Cyber Security Centre – Guidance on choosing, configuring and deploying video conferencing

UK Safer Internet Centre – Guidance on safe remote learning

Online safety – support for children

Childline – For free and confidential advice

UK Safer Internet Centre – To report and remove harmful online content

CEOP Safety Centre – to report online child sexual abuse

Online safety- parental support

Childnet – Offers a toolkit to support parents and carers of children of any age to start discussions about their online life, and to find out where to get more help and support

Commonsensemedia – Provides independent reviews, age ratings, & other information about all types of media for children and their parents

Government advice – About protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying

Internet Matters – Provides age-specific online safety checklists, guides on how to set parental controls, and practical tips to help children get the most out of their digital world

How Can I Help My Child? – Marie Collins Foundation – Sexual abuse online

London Grid for Learning – Provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online

Stopitnow resource from The Lucy Faithfull Foundation – Can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)

CEOP Education – Provides information, guidance and resources for support for parents and carers, helping them to protect their child(ren) from online sexual abuse

Parentzone – Provides help for parents and carers on how to keep their children safe online

Talking to your child about online sexual harassment: A guide for parents – This is the Children's Commissioner's parental guide on talking to their children about online sexual harassment.