At Knights Enham Schools we provide…

Inclusive and ambitious learning experiences where our school community feels safe and motivated to achieve their best.

'Together We Achieve'

E-Safety Policy

Approved: November 2025

Review: November 2026

The internet, and devices that utilise it, are now part of everyday life for most people and a powerful and useful tool for pupils' learning. It is the entitlement of every pupil to have access to the internet and digital technologies, in order to enrich his/her learning. The use of the internet is also part of the Computing National Curriculum.

Aims

All pupils will:

- learn to use the internet and other digital technologies safely and responsibly
- use the internet and other digital technologies to support, extend and enhance their learning
- develop an understanding of the uses, importance and limitations of the internet and other digital technologies
- develop a positive attitude to the internet and develop their ICT capability and confidence through both independent and collaborative working
- develop an understanding of intellectual property and copyright
- learn how to use the internet safely and how to act if they come across something inappropriate

Pupils' use of the internet

All pupils will:

- be taught how to effectively use the internet for research purposes
- be taught to evaluate information on the internet
- be taught how to report inappropriate web content
- use the internet to enhance their learning experience
- be taught how to use emails through Purple Mash (computing scheme of work)
- have opportunities to engage in independent and collaborative learning using the internet and other digital technologies
- only be permitted to have mobile phones or other personal handheld technology in school with the permission of the headteacher. These pupils will be required to follow the expectations stated in the ICT Acceptable Use Agreement, and sign a pupil-friendly version

Staff responsibilities and actions

All **staff, volunteers, governors and other adults working at the school** must model appropriate behaviour in relation to use of the internet and must sign the ICT Acceptable Use Agreement before using any information communications technology on site. All staff should:

- contribute to the development of E-Safety policies and practices
- staff ensure that children are supervised when using the internet
- take responsibility for the security of confidential data
- actively teach the pupils about E-Safety during each unit of learning that involves online use
- regularly teach E-Safety to highlight to the children the importance of being safe on the internet and help children understand what to do

- refer to the e-safety class posters to help children understand what to do when they come across something inappropriate
- explain to children what internet use is acceptable, and will ensure that pupils only access material that is appropriate to their age and maturity
- set clear Learning Aims and expectations of use for internet use during lessons, and ensure that internet use is embedded to support and enhance the whole curriculum demonstrate safe access to the web, and ensure that all pupil access is supervised
- deal with E-Safety issues as they arise and be alert to potential issues / risks
- report to the DSL/headteacher if inappropriate website is accessed

Headteacher and DLS responsibilities

The headteacher and DSL will

- assume overall responsibility for E-Safety issues within the school but will delegate the day-to-day responsibility to the Computing lead or DSL
- review the security of the school information systems and users regularly
- provide guidance and resources to support other staff's use of the internet and digital technologies / devices
- provide support for parents/carers through newsletters, meetings
- liaise with IT support company ensuring effective filtering is set and monitored
- ensure that developments at Local Authority level are communicated to relevant staff
- ensure that the Governing Body is informed of e-safety issues and policies.
- make all staff aware that internet traffic can be monitored and traced to the individual user, and that safe, professional conduct is essential
- assume editorial responsibility for all content on the school website, Facebook page, Twitter account and YouTube channel, ensuring that it is accurate, appropriate and accessible
- report any material believed to be illegal to appropriate agencies such as the Internet Watch Foundation (IWF) or Child Exploitation and Online Protection Centre (CEOP).

Responsibilities: Governors

- Our Governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the Governors (or a Governors' subcommittee) receiving regular information about e-safety incidents and monitoring reports

Risks

As identified in Annex 7 of our Child Protection policy, risks can be categorised into 4 main areas:

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

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

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

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

Email

- Pupils only use emails via Purple Mash. Internal to peers only – content checked and authorised by class teachers.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
- Staff use only the school email services to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Emails sent to external organisations must be written carefully and professionally

Publishing web content

- The contact details on the school website should be the school address, admin office email address and telephone number
- The website should respect and reflect property rights and copyright
- Images of pupils should be selected carefully and be published only with the consent of the parents/carers and be presented in a way that reduces the opportunities for it to be reused elsewhere

Managing social media

Children using social media will be advised:

- to discuss their account on an ongoing basis with a trusted adult in their family
- never to give out personal details which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM and email addresses, full names of friends/family, specific interests and clubs
- not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- not to publish photos of themselves or others online
- not to arrange to meet people who they have met online

School social media:

- The school's Facebook page and Twitter account are managed by the headteacher.
- All personal information, including names and photos of pupils will only be published with specific and informed parental consent. In general, the least that can be shared the safer the post.
- Any staff content on the school website must be agreed with the Headteacher.

Staff use of social media:

- Staff are advised to exercise extreme care in their personal use of social networking sites, giving consideration to their professional role working with children
- Staff should make appropriate use of the security settings available
- Staff are advised that inappropriate communications that come to the attention of the school can lead to disciplinary action, including dismissal Under no circumstances should any school staff have any pupils or any ex-pupils under the age of 18 as friends on their social networking sites
- School staff are strongly advised not to accept friendships via their social networking with parents, ex-parents and governors. Where staff do accept such friendships, they must not engage in any discussion regarding the school whether expressing personal views or opinions or simply recounting events or stating facts
- School staff are fully entitled to accept friendships with colleagues via their social networking site but should take care in communications exchanged in areas of public access
- The Leadership Team and those who have line management responsibility are advised to consider the appropriateness of accepting colleagues as contacts on social networking sites
- Staff to share any concerns that may arise on social media with Headteacher

Internet filtering

- The school will work with Harrap IT Team to ensure that systems to protect pupils are reviewed and improved
- If staff or pupils discover unsuitable sites, the URL must be reported by the teacher to the headteacher or DSL immediately.
- The school's broadband access will be filtered according to the age and maturity of pupils.

Managing emerging technologies

New IT applications, both hardware and software, will initially be explored by the Digital Leader. Advice will then be put to the Leadership Team, enabling them to assess the educational benefits and potential risks.

Training

The school will ensure that all teaching staff (teachers and learning support assistants) have a basis understanding of E-Safety. Formal training will be provided for key staff. Ongoing dialogue will support an open culture where potential issues are identified, discussed and solutions agreed.

Parent and carer awareness

Parents and carers may have a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- offer occasional E-Safety workshops / newsletters / advice for parents/carers
- share with parents/carers materials that will support their understanding of social media
- Links to https://www.ceopeducation.co.uk/parents/ , https://www.nspcc.org.uk/keeping-children-safe/online-safety/ and https://saferinternet.org.uk/guide-and-resource/parents-and-carers can be found on our website, within the Safeguarding page.

E-Safety Complaints

Instances of pupil internet or Learning Platform misuse should be reported to a member of staff

Staff must log incidents reported to them and if necessary, refer the matter to a senior member of staff

Instances of staff internet or other ICT misuse should be reported to, and will be dealt with by, the Headteacher

Related policies

This policy should be read in conjunction with the school's ICT Acceptable Use Agreement, Behaviour policy, Child Protection Policy and Confidentiality Policy. Any complaints relating to E-safety will be managed according to the school's Complaints Policy.

E-Safety in Classrooms

Each term or lessons when using the internet children will be reminded by teachers how to stay safe on the internet. Every classroom will display an E-Safety poster which children can refer to and help guide them in situations.

Appendix 1

ICT Acceptable Use Agreement for Staff

To ensure that members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's policy for Internet access for further information and clarification.

- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I understand that I must not use the school ICT system to access inappropriate content

- I appreciate that ICT includes a wide range of systems, including mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that school information systems and hardware may not be used for private purposes without specific permission from the Head Teacher.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own.
- I will not install any software or hardware without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely. It must NOT be kept on removable storage devices.
- I will respect copyright and intellectual property rights.
- understand use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.
- I will report any incidents of concern regarding children's safety to the schools e-Safety Coordinator, the Designated Child Protection Liaison Officer or Head Teacher.
- I will ensure that electronic communications with parents via email, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing. The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. I have read, understood and accept the Staff Code of Conduct for ICT.

ICT Acceptable Use Agreement for Pupils E-Safety Rules

Key Stage 1

Think then Click

These rules help us to stay safe on the Internet:

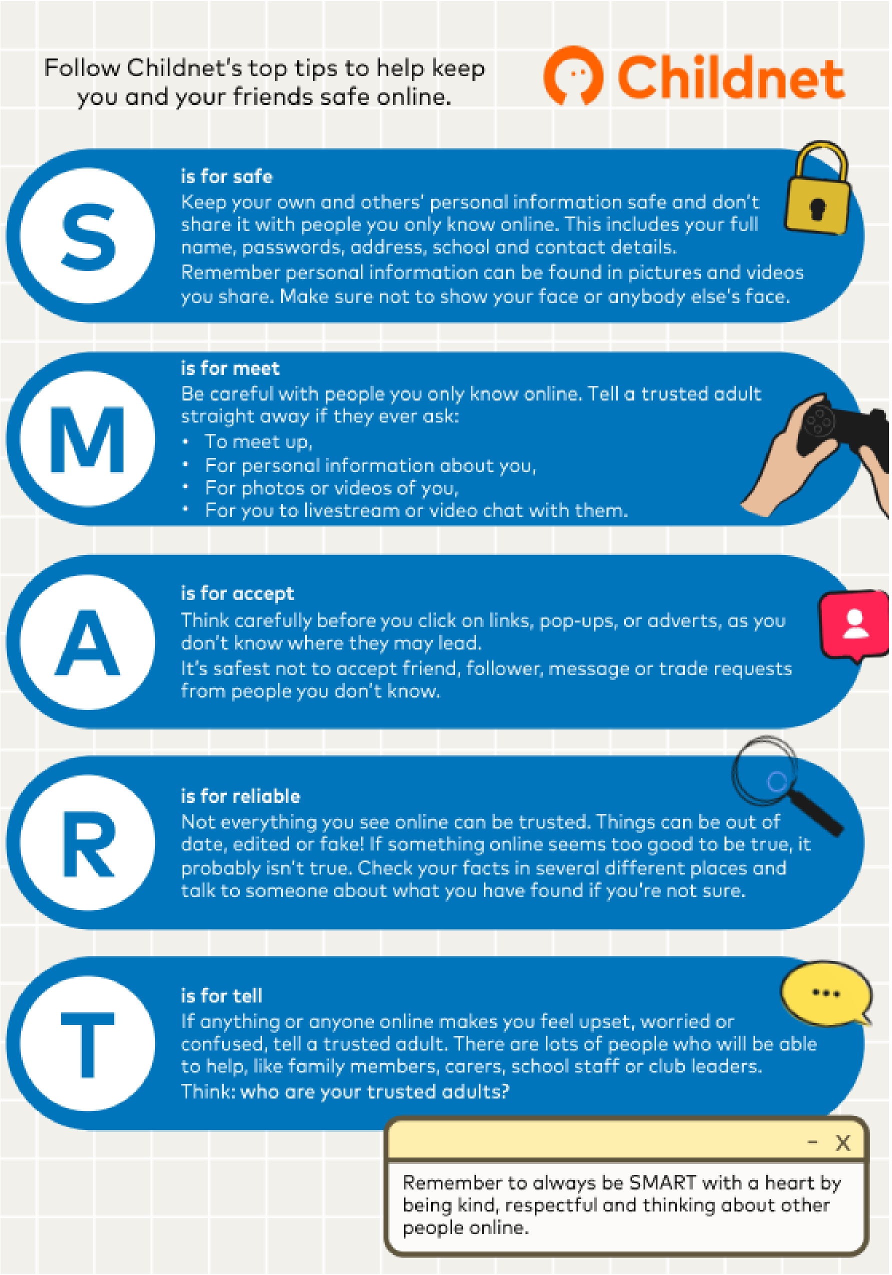
- We only use the internet when an adult is with us.
- We can send and open emails together.
- We always ask if we get lost on the Internet.
- We can click on the buttons or links when we know what they do.
- We can write polite and friendly emails to people that we know.
- I know I should never share personal information like my name, address or passwords with anyone.
- I know that if I see anything online that I don't like or understand I will tell and adult.

Key Stage 2

Think then Click

- We ask permission before using the Internet.
- We only use websites that an adult has chosen.

- We only use safe search sites when browsing.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any web page we are not sure about.
- We only message or email people an adult has approved.
- We send e-mails or messages that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone we don’t know.
- We do not open e-mails or messages sent by anyone we don’t know.
- We do not use Internet chat rooms.
- We only use age-appropriate apps.
- We try hard to keep our identity safe online.



Follow Childnet’s top tips to help keep you and your friends safe online.

Childnet

S is for safe
Keep your own and others’ personal information safe and don’t share it with people you only know online. This includes your full name, passwords, address, school and contact details.
Remember personal information can be found in pictures and videos you share. Make sure not to show your face or anybody else’s face.

M is for meet
Be careful with people you only know online. Tell a trusted adult straight away if they ever ask:

- To meet up,
- For personal information about you,
- For photos or videos of you,
- For you to livestream or video chat with them.

A is for accept
Think carefully before you click on links, pop-ups, or adverts, as you don’t know where they may lead.
It’s safest not to accept friend, follower, message or trade requests from people you don’t know.

R is for reliable
Not everything you see online can be trusted. Things can be out of date, edited or fake! If something online seems too good to be true, it probably isn’t true. Check your facts in several different places and talk to someone about what you have found if you’re not sure.

T is for tell
If anything or anyone online makes you feel upset, worried or confused, tell a trusted adult. There are lots of people who will be able to help, like family members, carers, school staff or club leaders.
Think: who are your trusted adults?

- X

Remember to always be SMART with a heart by being kind, respectful and thinking about other people online.