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

(based on a model policy from Hampshire County Council)

Approved: September 2026

Date of next review: September 2027

E-Safety Policy

1 Purpose and scope

The internet and digital technology are integral to learning, communication and school operations. The federation is committed to enabling pupils and staff to use technology confidently, creatively and safely while protecting children from harm.

Online safety is a safeguarding responsibility. This policy applies to all pupils, staff, governors, volunteers, contractors and visitors; to school-managed devices and services wherever used; and to personal devices or accounts when their use affects the safety, welfare, reputation or operation of the schools.

This policy has been updated with regard to Keeping Children Safe in Education 2026, the DfE filtering and monitoring core standard updated in September 2026, statutory mobile-phone guidance applying from September 2026, DfE guidance on generative AI, and Hampshire Safeguarding Children Partnership procedures.

2 Aims

- teach pupils to use technology safely, respectfully, responsibly and critically
- support learning while reducing exposure to illegal, inappropriate and harmful content or contact
- ensure concerns are recognised, recorded and responded to promptly as safeguarding matters
- set clear responsibilities for governance, leadership, safeguarding, IT support, staff, pupils and families
- protect personal data, privacy, intellectual property and the integrity of school systems

3 The four areas of online risk

The federation uses the four areas of risk described in Keeping Children Safe in Education:

Area	Examples
Content	Exposure to illegal, inappropriate or harmful material, including pornography, misinformation and disinformation, misogyny, racism, antisemitism, self-harm, suicide, radicalisation, extremism and AI-generated material.
Contact	Harmful interaction with others, including peer pressure, bullying, grooming, exploitation, impersonation and adults posing as children.
Conduct	Behaviour that causes or increases harm, including cyberbullying and the creation, consensual or non-consensual sharing, or threatened sharing of nude or semi-nude images. This includes images digitally altered or wholly generated using AI, such as deepfakes or deep nudes.
Commerce	Risks including inappropriate advertising, phishing, scams, financial exploitation, gambling and in-app purchases.

4 Roles and responsibilities

Governing body

- holds overall strategic responsibility for online safety and for appropriate filtering and monitoring

- appoints a responsible governor and receives assurance, including the recorded annual review, checks, incidents, actions and training
- ensures online safety is embedded in safeguarding, curriculum, behaviour, staff conduct, data protection and technology policies
- ensures the DSL has appropriate status, authority, time, training and resources

Executive Headteacher and senior leadership team

- implement this policy and allocate clear safeguarding and technical responsibilities
- scope the federation's needs, procure suitable systems and document decisions about content that is blocked, allowed or exceptionally released
- ensure staff understand their responsibilities and are trained to report and act on concerns
- approve and document any temporary filtering exception after the DSL has considered safeguarding implications
- ensure a risk assessment is completed before introducing new technology, including generative AI

Designated Safeguarding Lead

- takes lead responsibility for online safety and works closely with SLT, the responsible governor and IT support
- reviews relevant monitoring reports and alerts, decides safeguarding action, and records decisions on CPOMS
- provides assurance that filtering and monitoring arrangements are effective and reviewed regularly
- recognises the additional online risks faced by pupils with SEND, communication needs, language barriers or other vulnerabilities
- follows the Child Protection Policy and Hampshire Safeguarding Children Partnership procedures, including referrals to statutory agencies where required

IT support provider

- maintains filtering and monitoring systems, security controls, accounts, updates and audit information
- provides reports and acts promptly on technical actions agreed with the DSL or SLT
- supports reviews and checks across both school sites and all user groups, networks, services and school-managed devices
- confirms that new devices and services are protected before deployment and that protection continues after significant changes

All staff, volunteers and contractors

- model safe and professional behaviour and follow the Staff Code of Conduct and Acceptable Use Agreement
- maintain active supervision; filtering does not replace professional vigilance
- teach and reinforce online safety whenever digital technology is used
- never investigate a safeguarding concern beyond what is necessary to establish basic facts
- report harmful content, suspicious activity, breaches or disclosures immediately to the DSL or deputy and record concerns on CPOMS in line with school procedure
- report concerns about an adult to the Headteacher; concerns about the Headteacher go to the Chair of Governors; allegations and low-level concerns follow the Child Protection Policy

5 Education and curriculum

Online safety will be taught progressively through Computing, Relationships and Health Education and other relevant curriculum areas. Teaching will be age-appropriate, inclusive and responsive to local and emerging risks. Pupils will learn how to verify information, recognise manipulation and scams, manage privacy and passwords, understand consent and respectful communication, report concerns, and respond safely if something worries or upsets them.

Teaching will include misinformation, disinformation, harmful online challenges, persuasive design, algorithms, AI-generated content and deepfakes. Pupils will be reminded that apparent realism does not prove that online material is genuine.

Staff will use clear learning intentions, suitable resources and active supervision. Pupils will be reminded of the SMART rules and trusted adults. The Childnet SMART poster remains displayed and used in classrooms.

6 Filtering and monitoring

Filtering is preventative and monitoring is reactive. Neither can guarantee safety, so both must operate alongside an effective curriculum, supervision, reporting routes and safeguarding response.

- The federation will maintain different, age- and role-appropriate profiles for pupils, staff and guests; a single blanket profile will not be used.
- Filtering will apply to all users and internet connections and, so far as technically possible, to all school-managed devices wherever used. Unmanaged devices using school internet access will use a separate, appropriately filtered network.
- Provider arrangements must implement and protect IWF and Counter-Terrorism Internet Referral Unit blocklists and address adult content, circumvention tools, VPNs, proxies, multilingual material, image, audio, video, app and AI-generated content.
- The DSL will review relevant alerts and reports. Access to monitoring information will be restricted to authorised staff and handled lawfully and proportionately.
- The federation will review filtering and monitoring at least once each academic year and additionally following a safeguarding risk, major incident, material system or network change, new device or service, new working practice, significant update, or introduction of generative AI.
- The recorded review will involve SLT, DSL, IT support and the responsible governor and will consider pupil age, SEND, EAL, vulnerability, curriculum need, digital resilience, incidents, off-site use and known technical limitations.
- Checks will be risk-based and recorded, stating the date, person completing the check, locations/devices/accounts tested, outcome and actions. Both sites and pupil, staff and guest profiles will be included.

7 Responding to incidents and disclosures

Any online concern may be a safeguarding concern even when it occurs away from school. Staff must listen, reassure, avoid blame, preserve evidence without viewing, copying or forwarding illegal imagery, and report immediately to the DSL or deputy. If a child is at immediate risk, emergency services must be contacted.

- Do not promise confidentiality. Explain that information will be shared only with people who need to help.
- Do not ask a pupil to delete material before the DSL has considered evidence and safety. Do not search a device or account unless authorised and acting in line with the school's Searching, Screening and Confiscation procedures.
- Suspected child sexual abuse material must not be printed, copied, downloaded, forwarded or deliberately viewed. The DSL will take advice and make referrals through appropriate safeguarding and law-enforcement routes.

- Reports involving nude or semi-nude images, including AI-generated or digitally altered images, will be managed under current safeguarding guidance and recorded as a safeguarding concern.
- Where conduct may constitute cyberbullying, discrimination, sexual harassment, criminal exploitation, radicalisation or another offence, the Child Protection and Positive Behaviour policies will also apply.
- Technical evidence and logs will be secured with support from authorised IT staff. Personal data will be shared only where necessary, proportionate and lawful.

8 Mobile phones, smartwatches and personal devices

In line with statutory DfE guidance applying from September 2026, pupils must not use mobile phones or other personal smart devices during the school day, including lessons, breaktimes, lunchtimes and school-led activities on site. Devices brought with permission for travel or an agreed individual need must be switched off and stored securely in accordance with school arrangements.

Reasonable, individual exceptions may be agreed by the Headteacher for medical needs, disability, safeguarding or another exceptional circumstance. These will be documented and reviewed. Pupils must not use personal devices to photograph, record or communicate during the school day unless specifically authorised for an educational or safety purpose.

Staff must keep personal phones out of use when supervising pupils except for an authorised operational or emergency purpose. Photography or recording of pupils must use school-approved devices and systems. Visitors will be informed of these expectations.

9 Generative artificial intelligence

Only tools approved by the federation may be used for school business or with pupils. Approval will consider educational purpose, age restrictions, safeguarding by design, filtering and monitoring compatibility, privacy, security, data residency and retention, intellectual property, accessibility, bias, accuracy and terms of service.

- Personal, special-category, safeguarding or confidential information must not be entered into a public or unapproved AI tool.
- Pupils will use generative AI only when directly authorised and supervised, with age-appropriate accounts and tasks.
- AI outputs must be checked by a competent person. They may contain errors, bias, fabricated sources or unsafe content and must not make safeguarding, admission, assessment, disciplinary or other high-impact decisions without accountable human judgement.
- AI-generated work must be acknowledged where required. Copyright, licensing and academic integrity requirements continue to apply.
- Any AI output that raises a safeguarding concern, including sexualised deepfakes, grooming, hateful material, self-harm content or impersonation, must be reported immediately under section 7.

10 Email, messaging and communication

- Pupils use only school-approved, age-appropriate communication tools, such as supervised Purple Mash email, for authorised learning.
- Staff use official school accounts and approved platforms for school business. Messages must be professional, necessary and capable of appropriate scrutiny.
- Staff must not use personal accounts, personal messaging services or social media to communicate privately with pupils.
- Suspicious links, attachments, requests for credentials, payment changes or personal information must be reported without interaction.

11 Social media, publication and images

Official content is published only through authorised school accounts. Website and social-media content must be accurate, appropriate, accessible and lawful. The school address, central office contact details and approved information will be used rather than personal contact details.

Images and information about pupils will be selected carefully and published only where the school has an appropriate lawful basis and has followed its privacy information and consent arrangements. Staff must consider whether contextual details, metadata, uniform, location or routines could identify or place a child at risk.

- Staff must not accept pupils or former pupils under 18 as contacts on personal social-media accounts.
- Staff should maintain professional boundaries with parents, carers, governors and colleagues and must not discuss confidential school matters on personal accounts.
- Online conduct outside work may be addressed under the Staff Code of Conduct where it affects safeguarding, professional suitability, confidentiality or trust in the school.
- Pupils are taught not to share personal or location information, meet online contacts, create or share harmful content, or respond to pressure; they should block, preserve evidence and tell a trusted adult.

12 Data protection, security and acceptable use

- Users must use their own account, protect passwords and multi-factor authentication, lock unattended devices and report suspected compromise immediately.
- Personal data must be stored and shared only through approved systems. Unapproved removable media, personal cloud storage and personal email must not be used for school data.
- Software, browser extensions, apps and hardware may be installed or connected only with authorisation.
- Users must respect copyright, licences and intellectual property and must not use school systems for illegal activity, gambling, personal financial gain, unauthorised political campaigning or commercial advertising.
- School systems, internet use, email and devices may be logged and monitored for safeguarding, security and compliance in accordance with law and school privacy information.

13 Training, induction and awareness

All staff will receive online-safety training at induction, including the expectations, roles and responsibilities for filtering and monitoring. Safeguarding and online-safety knowledge will be updated at least annually and more often when risks, technology or guidance change. The DSL and deputies will maintain up-to-date knowledge of online harms and the additional risks faced by pupils with SEND.

Parents and carers will be supported through school communications, the safeguarding pages of the website and, where helpful, workshops. Information will include age restrictions, device controls, reporting routes, scams, social media, gaming, AI and how to talk with children about online experiences.

14 Monitoring, recording and review

Safeguarding incidents and decisions will be recorded on CPOMS in accordance with the Child Protection Policy. Technical checks, filtering changes and annual review actions will be recorded separately and made available to governors and inspectors as appropriate. Patterns and inequalities, including risks affecting pupils with SEND or other vulnerabilities, will inform training, curriculum and controls.

This policy will be reviewed at least annually and sooner following a serious incident, identified gap, legal or guidance change, introduction of significant technology, or material change to filtering and monitoring. Review does not wait for the stated date where action is required.

15 Related policies and guidance

- Child Protection and Safeguarding Policy
- Positive Behaviour Policy
- Staff Code of Conduct and low-level concerns procedures
- Data Protection Policy, privacy notices and records management arrangements
- Acceptable Use Agreements
- Searching, Screening and Confiscation procedures
- Remote learning, photography and social-media arrangements
- Keeping Children Safe in Education 2026
- DfE Filtering and Monitoring Core Standard (updated September 2026)
- DfE Mobile Phones in Schools statutory guidance (from September 2026)
- DfE Generative Artificial Intelligence in Education and product safety expectations
- Teaching Online Safety in Schools
- Hampshire Safeguarding Children Partnership procedures

Appendix 1 Staff acceptable use agreement

I understand and agree that I will:

- follow this policy, the Staff Code of Conduct and safeguarding procedures
- use only authorised accounts, devices, software and services for school business
- keep credentials secure and never use another person's account
- protect personal and confidential information and use approved storage and communication systems
- maintain professional boundaries in all digital communication
- actively supervise pupils and report any concern, accidental access, breach, suspicious activity or weakness immediately
- not deliberately access, create, store or share illegal, sexual, hateful, extremist or otherwise inappropriate material
- not enter personal, confidential or safeguarding information into unapproved generative AI tools
- check AI-generated content and remain accountable for all professional work and decisions
- respect copyright and intellectual property
- understand that authorised logging and monitoring may take place for safeguarding, security and compliance

Name	
Role	
Signature	
Date	

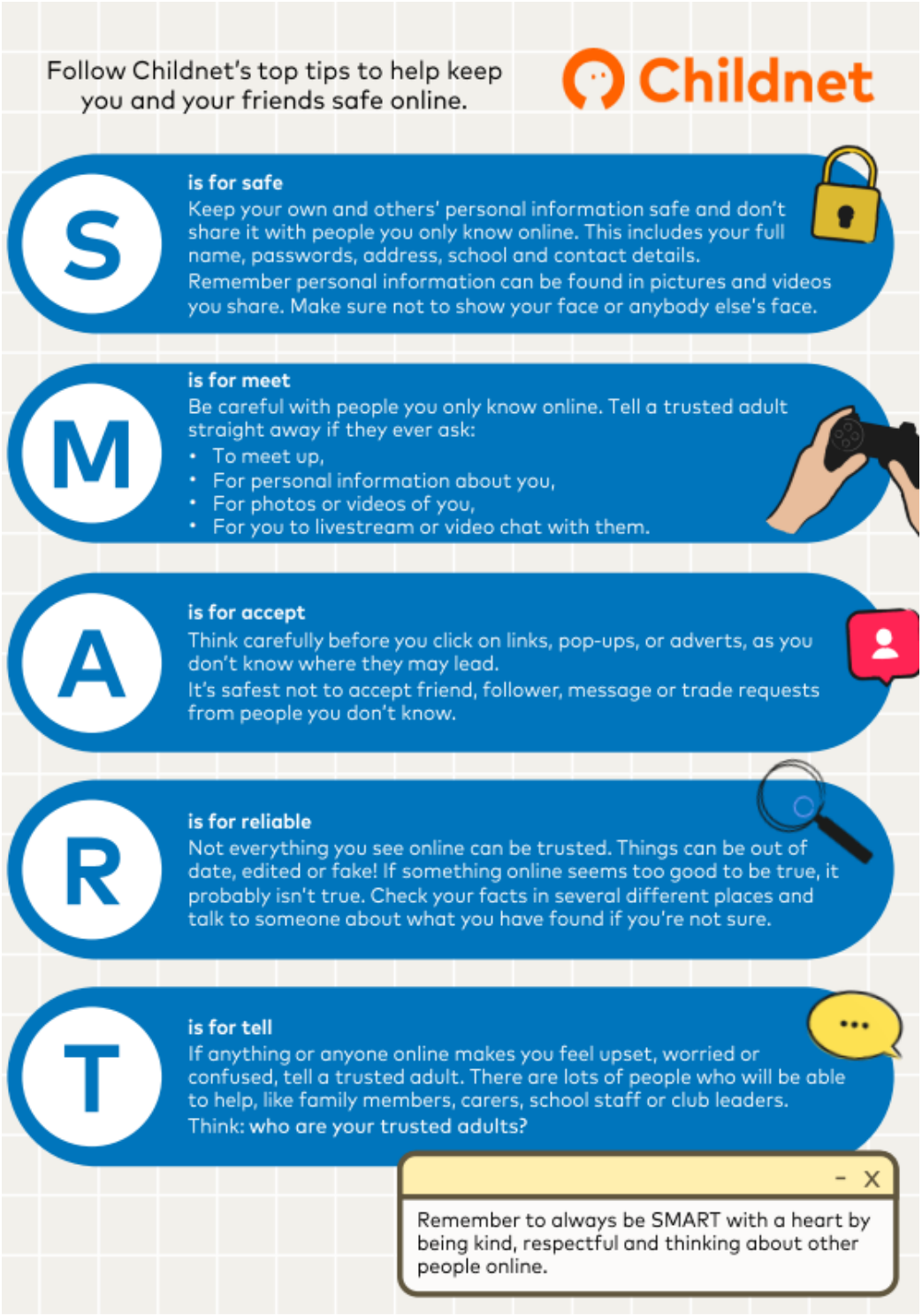
Appendix 2 Pupil online safety rules

Nursery and Key Stage 1

- I use the internet with an adult.
- I ask before I click, send or open something.
- I keep my name, address, school, passwords and other personal information private.
- I am kind and respectful online.
- If anything worries, confuses or upsets me, I stop and tell a trusted adult.
- I know pictures and videos, including AI pictures, may not be real.

Key Stage 2

- I use only approved websites, apps, accounts and devices for the task.
- I protect passwords and personal information and do not try to bypass school safety controls.
- I check information using reliable sources and remember that online and AI-generated content can be false or manipulated.
- I communicate respectfully and do not create, request, share or forward harmful, bullying, sexual or embarrassing content.
- I do not arrange to meet an online contact or respond to pressure, threats, scams or requests for images.
- If I see something unsafe, I stop, do not share it, preserve the evidence where safe, and tell a trusted adult immediately.
- I do not use my mobile phone or personal smart device during the school day.


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