

[illegible]

High Expectations, High Ercall

Read alongside: Child Protection and Safeguarding Policy; ICT and Internet Acceptable Use Policy; Safe Use of Technology – Mobile Phones and Smart Technology Policy; AI Policy; Behaviour and Anti-Bullying Policy; Child-on-Child Abuse Policy; Staff Code of Conduct; Data Protection Policy; Computing and PSHE/RSE curriculum documentation.

1. Aims and principles

High Ercall Primary School recognises that technology is an essential part of education and modern life. Our aim is to enable pupils to benefit from digital technology while providing a calm, safe and supportive online environment. Online safety is a safeguarding responsibility and a running, interrelated theme across safeguarding, curriculum, behaviour, staff conduct, parental engagement, filtering and monitoring, mobile technology and artificial intelligence (AI).

- Maintain robust systems to protect pupils, staff, volunteers and governors online.
- Identify and support pupils who may be at greater risk of online harm, including vulnerable pupils, victims of abuse and pupils with SEND.
- Teach pupils the knowledge, critical thinking, behaviours and practical skills needed to use technology safely, respectfully, responsibly and securely.
- Ensure clear processes for identifying, reporting, recording, escalating and learning from online safety concerns.
- Balance effective safeguarding controls with pupils' entitlement to learn how to assess and manage online risk.

2. The four categories of online risk

High Ercall uses the four categories in Keeping Children Safe in Education (KCSIE) 2026 as the foundation of its online safety approach:

Risk	Examples
Content	Illegal, inappropriate or harmful content, including pornography, racism, misogyny, antisemitism, self-harm, suicide, radicalisation, extremism, misinformation, disinformation and conspiracy theories.
Contact	Harmful interaction with others, including peer pressure, commercial contact and adults posing as children or young adults to groom or exploit pupils for sexual, criminal, financial or other purposes.
Conduct	Online behaviour that increases the likelihood of harm, including online bullying, abusive or misogynistic messages, creating/sending/receiving explicit images, non-consensual sharing of nudes or semi-nudes, and AI-generated or digitally altered intimate images/deepfakes.
Commerce	Online gambling, inappropriate advertising, phishing, fraud, financial scams and other commercial exploitation.

3. Legislation and guidance

This policy reflects current statutory and Department for Education guidance for the 2026–27 academic year, including:

- Keeping Children Safe in Education 2026 (in force from 1 September 2026).
- DfE filtering and monitoring core standard, updated June 2026, and the wider digital and technology standards.
- DfE guidance on generative AI in education and the 2026 Generative AI Product Safety Standards.
- DfE guidance on teaching online safety, cyber security, searching/screening/confiscation, behaviour and mobile phones in schools.
- Education Act 1996; Education and Inspections Act 2006; Education Act 2011; Equality Act 2010; UK GDPR and Data Protection Act 2018 as amended, including relevant 2026 data-protection changes.
- National Curriculum computing requirements and statutory Relationships Education and Health Education requirements for primary schools.

4. Roles and responsibilities

4.1 Governing Body

- Hold the Headteacher to account for effective implementation of this policy and ensure online safety is embedded across safeguarding arrangements.
- Ensure appropriate filtering and monitoring systems are in place and their effectiveness is reviewed at least once every academic year.
- Receive assurance about online safety risks, incidents, training, filtering/monitoring, vulnerable groups and actions taken.
- Ensure staff receive safeguarding training that includes online safety and understand their filtering and monitoring responsibilities.
- Ensure teaching about safeguarding, including online safety, is adapted where necessary for vulnerable pupils, victims of abuse and pupils with SEND.

4.2 Headteacher

- Ensure this policy is understood and implemented consistently across school.
- Ensure sufficient resources, training and technical support are available.
- Ensure online safety is considered when new technology, platforms, EdTech or AI tools are introduced.

4.3 Designated Safeguarding Lead (DSL)

- Take lead responsibility for safeguarding and child protection, including online safety and understanding the filtering and monitoring systems and processes in place.
- Respond to safeguarding concerns identified through online activity or filtering/monitoring alerts and ensure appropriate recording on CPOMS.

- Work with the Headteacher, Computing/Online Safety Lead and IT provider to review online risks and filtering/monitoring effectiveness.
- Provide safeguarding and online safety updates to staff and appropriate assurance to governors.

4.4 Computing / Online Safety Lead

- Coordinate the online safety curriculum and support staff to teach online safety progressively across EYFS–Year 6.
- Work with the DSL and Headteacher to analyse trends, SENSO reports and emerging risks and to strengthen curriculum provision.
- Support annual policy review, staff development and the school's online safety self-review processes.

4.5 IT provider

- Telford & Wrekin Council / the school's commissioned IT provider has technical responsibility for maintaining relevant network, security, filtering and monitoring services in accordance with agreed service arrangements.
- Support the school to investigate technical concerns, test systems and implement changes following review or identified risk.

4.6 All staff, contractors and volunteers

- Read, understand and implement this policy and the relevant Acceptable Use Agreement.
- Model safe, responsible and professional technology use.
- Maintain professional curiosity: online harm may occur alongside face-to-face abuse.
- Know how to report safeguarding concerns, filtering/monitoring failures and inappropriate or harmful content; when unsure, speak to the DSL or deputy DSL.
- Never investigate safeguarding concerns beyond their role or view/share suspected illegal child sexual abuse imagery.

4.7 Parents/carers and pupils

- Parents/carers are encouraged to work in partnership with school, discuss online safety at home and raise concerns promptly.
- Pupils are expected to follow age-appropriate Acceptable Use Agreements; report worries promptly and treat others respectfully online as well as offline.

5. Educating pupils about online safety

Online safety is taught through a progressive programme across computing, PSHE/Relationships Education and other curriculum opportunities. High Ercall will use appropriate resources such as ProjectEVOLVE, Natterhub, UK Safer Internet Centre/Childnet resources and other quality-assured materials. Teaching is revisited in response to emerging risks and school incidents.

- Use technology safely and respectfully; keep personal information private; know where and how to seek help.

- Recognise acceptable and unacceptable online behaviour and understand that the same standards of kindness, respect and responsibility apply online and offline.
- Understand privacy, digital footprints, location sharing, passwords and account security.
- Evaluate online information critically, including misinformation, disinformation, manipulated media, search results, advertising and AI-generated content.
- Understand that online identities may be false and recognise grooming, exploitation, coercion, scams and pressure.
- Understand cyberbullying, harassment, harmful sexual behaviour and the risks of creating, requesting, sharing or forwarding nudes/semi-nudes or AI-generated/digitally altered intimate images.
- Know how to block, report, preserve evidence appropriately and seek help from a trusted adult.
- Develop age-appropriate cyber-security knowledge, including strong passwords, phishing/social engineering, suspicious links and reporting security concerns.

Teaching will be adapted where necessary for pupils with SEND, communication needs, previous experiences of abuse or other vulnerabilities. Staff will consider what additional explanation, repetition, supervision or personalised teaching is required.

6. Artificial intelligence (AI) and emerging technology

Generative AI can support education but may also create safeguarding, data-protection, intellectual-property and accuracy risks. High Ercall's separate AI Policy sets out detailed expectations; this section establishes the online-safety requirements.

- Pupil use of generative AI in school will only take place where the school has approved the tool/use case, age restrictions are met, appropriate safeguards are in place and use is supervised at a level appropriate to the pupils.
- Staff must not enter personal, special-category, safeguarding or confidential school information into unapproved AI systems.
- AI output must be critically checked; pupils will be taught that confident-sounding outputs may be inaccurate, biased, fabricated or unsafe.
- The school will consider safeguarding, ethics, privacy, data protection, intellectual property, age assurance, filtering and monitoring when assessing new AI tools.
- AI-generated bullying, impersonation, deepfakes and sexualised or intimate imagery will be treated as serious safeguarding/behaviour concerns and referred to the DSL.
- Filtering and monitoring reviews will explicitly consider generative AI, including whether AI services or dynamic/generated content create gaps in current controls.

7. Filtering and monitoring

High Ercall uses layered filtering and monitoring. At the time of this policy, internet filtering is provided through Telford & Wrekin Council services, including Smoothwall, and school device monitoring uses

SENSO where supported. Technical arrangements may change during the policy period; the safeguarding standard below remains the requirement.

- Filtering must block illegal, inappropriate and harmful content without unreasonably restricting teaching, learning or school administration.
- Monitoring must support timely identification and response to safeguarding concerns; it complements rather than replaces active staff supervision.
- All relevant staff must know how to report suspected unsuitable access, over-blocking, under-blocking, system failure, circumvention attempts (such as VPN/proxy use) and unusual activity caused by legitimate teaching.
- Where SENSO is available, alerts/reports will be reviewed regularly by designated staff and safeguarding concerns escalated to the DSL and recorded on CPOMS as appropriate.
- Where monitoring software does not cover a device or service, including any identified iPad or app limitation, staff supervision and other controls must be strengthened accordingly.

7.1 Annual effectiveness review

In line with KCSIE 2026, the effectiveness of filtering and monitoring will be reviewed at least once every academic year. The review will be led by the SLT member responsible for filtering and monitoring, supported by the DSL and IT support, and will involve the responsible governor as part of governance assurance.

- Check filtering is working appropriately on all internet-connected devices and in all relevant school locations, including guest access and any backup connection where applicable.
- Keep a written record of the checks and review findings, identified gaps, actions, owners and completion dates.
- Consider pupil age, SEND and vulnerability profiles, patterns of incidents, new technologies and generative AI risks.
- Review sooner where a safeguarding risk is identified, working practice changes, a significant incident occurs or new technology is introduced.
- Use appropriate testing tools and provider assurance to check blocking of illegal child sexual abuse material, unlawful terrorist content and other harmful/inappropriate content.

We meet the digital and technology standards laid out by the DfE in the following ways:

Standard	Our actions
Identify and assign roles and responsibilities to manage your filtering and monitoring systems	Telford and Wrekin Council have technical responsibility for: • maintaining filtering and monitoring systems • providing filtering and monitoring reports • completing actions following concerns or checks to systems The designated safeguarding lead takes lead responsibility for • understanding the filtering and monitoring systems and

	processes in place overseeing and acting upon filtering and monitoring reports, safeguarding concerns and checks to filtering and monitoring systems The DSL / Computing Lead monitor the systems in school. Lead Governor: Fara Gater It is the responsibility of all teaching staff/teaching assistants to ensure that they observe throughout computing sessions. All staff will receive training on the expectations, roles and responsibilities in relation to filtering and monitoring.
Review your filtering and monitoring provision at least annually	The review will identify our current provision, any gaps and take account of the specific needs of our pupils and staff. Governing bodies and proprietors ensure that filtering and monitoring provision is reviewed, which can be part of a wider online safety review, at least annually. The review will be conducted by members of the senior leadership team, the designated safeguarding lead (DSL), and the IT service provider and involve the responsible governor. The results of the online safety review will be recorded for reference and made available to those entitled to inspect that information. The review will take place annually or when a safeguarding risk is identified, there is a change in working practice or if new technology is introduced. We use South-West Grid for Learning's (SWGfL) testing tool to check that our filtering system is blocking access to: - illegal child sexual abuse material - unlawful terrorist content - adult content
Ensure your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning.	Our filtering provider is Smoothwall, through T&W Local Authority Internet Services. An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not: - unreasonably impact teaching and learning or school administration - restrict students from learning how to assess and manage

	risk themselves Our filtering provider is: • a member of Internet Watch Foundation (IWF) • signed up to Counter-Terrorism Internet Referral Unit list (CTIRU) • blocking access to illegal content including child sexual abuse material (CSAM) Our filtering system is operational, up to date and applied to all: • users, including guest accounts • school owned devices • devices using the school broadband connection Our filtering system: • filters all internet feeds, including any backup connections • is age and ability appropriate for the users, and is suitable for educational settings • handles multilingual web content, images, common misspellings and abbreviations • identifies technologies and techniques that allow users to get around the filtering such as VPNs and proxy services and block them • provides alerts when any web content has been blocked All staff are aware of reporting mechanisms for safeguarding and technical concerns. They should report if: • they witness or suspect unsuitable material has been accessed • they can access unsuitable material • they are teaching topics which could create unusual activity on the filtering logs • there is failure in the software or abuse of the system • there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks • they notice abbreviations or misspellings that allow access to restricted material If the filtering and monitoring system alerts staff to a concern the following actions may be taken if necessary: 1. A discussion with the class teacher or supervising staff to ascertain wider context, such as a legitimate reason for the alert. 2. DSL or Deputy DSL informed, should there not be a valid reason for the flagged concern. 3. Incident logged on the safeguarding system CPOMS.
--	---

	4. Following conversations with the child(ren), a consequence, increased monitoring or withdrawal of device use outside of the classroom. 5. Parents of the responsible child informed. 6. Additional teaching through e-safety and computing to address the issue. 7. Weekly SENSO reports are analysed to ensure the filtering and monitoring systems are not unnecessarily preventing access to sites required for teaching and learning.
Have effective monitoring strategies that meet the safeguarding needs of your school	Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software. Monitoring allows us to review user activity on school devices. For monitoring to be effective it must pick up incidents urgently, through alerts or observations, allowing us to take prompt action and record the outcome. Our monitoring strategy is informed by the filtering and monitoring reviews reported via SENSO each week. A variety of monitoring strategies are required to minimise safeguarding risks on internet connected devices and include: • physically monitoring by staff in classes watching screens of users • live supervision by staff on a console with device management software • network monitoring using log files of internet traffic and web access • individual device monitoring through software or third-party services In particular reference to iPads, monitoring is not provided by SENSO therefore children's use is monitored closely by supervising staff.

8. Managing internet and school technology access

- Pupils have supervised, age-appropriate access to internet resources using school-managed devices and accounts.
- Staff will check resources before planned use where reasonably practicable and use professional judgement about live/dynamic content.

- If unsuitable content appears, pupils should stop, close/minimise the content where safe to do so and tell an adult immediately. Staff should preserve safeguarding evidence appropriately without unnecessary viewing or sharing.
- Messaging or communication tools may only be used by pupils where explicitly approved for educational purposes and appropriately supervised.
- School internet and device activity may be filtered, monitored and investigated where necessary for safeguarding, security and compliance.

9. Mobile phones, smart technology and personal devices

High Erccall is a mobile-phone-free environment for pupils by default, consistent with KCSIE 2026 and the school's Safe Use of Technology Policy. Pupils are not permitted to have personal mobile phones or communicating/image-capable smart devices available for use during the school day.

- Where a parent requests that a phone is brought for journey/personal-safety reasons, prior permission must be obtained and the device handed to the school office immediately on arrival.
- Reasonable adjustments or medical exceptions will be made where required, documented and risk assessed.
- Staff personal-device use is governed by the Safe Use of Technology Policy and Staff Code of Conduct; personal devices must not be used to photograph or record pupils.
- Personal devices are not permitted on trips/residential for pupils unless an exceptional, documented arrangement has been authorised.

10. Cyberbullying, child-on-child abuse and harmful online behaviour

Online abuse may occur independently or alongside face-to-face harm. Staff will maintain an "it could happen here" approach and will not dismiss harmful behaviour as banter, joking or an inevitable part of growing up.

- Cyberbullying and online harassment will be addressed under the Behaviour and Anti-Bullying Policy and recorded appropriately.
- Sexual violence, sexual harassment, sharing nudes/semi-nudes, AI-generated sexualised imagery, coercion, exploitation or other child-on-child abuse will be managed under safeguarding and Child-on-Child Abuse procedures, led by the DSL.
- The school may respond to online behaviour outside school where it affects pupils, safeguarding, relationships, the orderly running of school or the welfare of the school community.
- Parents/carers will normally be informed of significant incidents involving their child unless doing so would create a safeguarding risk or conflict with agency advice.

11. Searching, confiscation and electronic evidence

Searching and confiscation will follow current DfE guidance and the school's Behaviour Policy. Only authorised staff will search a pupil or device where lawful and appropriate.

- If a device may contain evidence of an offence, staff will not delete relevant material and will seek DSL/police advice as appropriate.
- If staff suspect a device contains a nude/semi-nude or sexual image of a child, including an AI-generated or digitally altered image, they must not intentionally view, copy, print, forward or share it. The device should be secured and the DSL informed immediately.
- The DSL will follow current UKCIS guidance on sharing nudes and semi-nudes and liaise with police/children's social care where required.

12. Staff use of technology and cyber security

- Staff will use school systems and work devices in accordance with the ICT and Internet Acceptable Use Policy and Staff Code of Conduct.
- Work devices must be secured with approved authentication, encryption and automatic locking; updates must be installed as required and devices must not be shared with family or friends.
- Passwords/passphrases must be strong and unique and must not be shared. The school will follow current cyber-security standards rather than relying solely on routine password expiry where this is not required by current technical guidance.
- Suspected phishing, malware, account compromise, data breach or device loss must be reported immediately through the school's agreed IT/data-protection process.
- Staff must use approved systems for school information and must not use personal accounts, unapproved cloud services or unapproved AI tools for confidential/pupil information.

13. Parents and carers

The school will work with parents/carers to promote consistent online safety messages. Information may be shared through newsletters, the website, workshops, parent meetings and targeted communication following emerging concerns.

- Parents will be made aware, in appropriate terms, of the school's filtering and monitoring arrangements and the sites/platforms pupils may be asked to use.
- Parents are encouraged to discuss age restrictions, privacy settings, online relationships, gaming, social media, scams, AI and reporting routes with their children.
- Concerns should be raised with the class teacher, Headteacher or DSL as appropriate.

14. Responding to online safety incidents

Responses will prioritise safeguarding, be proportionate to the seriousness and context of the incident, and take account of age, SEND, vulnerability, intent, impact and previous concerns.

- Immediate safeguarding risk: make the child safe and contact the DSL/deputy DSL without delay.
- Technical/filtering concern: report through the school's IT route and inform the DSL where safeguarding may be involved.
- Record safeguarding/behaviour concerns on CPOMS in line with school procedures.
- Preserve evidence appropriately and avoid unnecessary viewing, copying or redistribution of harmful/illegal material.
- Seek advice/support from the local authority, IT provider, UK Safer Internet Centre, police, children's social care or other agencies where appropriate.
- Use incidents and near misses to inform teaching, supervision, filtering/monitoring settings, staff training and policy review.

15. Training

- All new staff receive safeguarding induction including online safety, filtering and monitoring responsibilities and reporting routes.
- All staff receive safeguarding/online safety updates at least annually and additional updates as risks, technology and guidance evolve.
- Governors receive appropriate online-safety and filtering/monitoring training to discharge their safeguarding responsibilities.
- The DSL and deputies maintain online-safety knowledge through statutory safeguarding training and regular updates.
- Training will include emerging risks such as generative AI, deepfakes, sextortion/scams, online misogyny, harmful content and methods used to circumvent controls.

16. Monitoring, review and governor assurance

The Computing/Online Safety Lead and DSL will monitor implementation using curriculum review, pupil/staff voice, CPOMS/incident themes, SENSO information where available, technical reports, filtering and monitoring checks, training records and the school's online safety self-review tools.

Area	Evidence	Frequency	Governor assurance
Filtering & monitoring	Recorded effectiveness review, device/location checks, provider reports, action plan	At least annually, sooner after change/risk	Systems appropriate; actions completed
Online incidents	CPOMS trends, cyberbullying/child-on-child abuse, technical incidents	Termly	Patterns, vulnerable groups and response reviewed
Curriculum	Planning, pupil voice, work scrutiny, SEND adaptation	At least annually	Progressive and responsive provision
Training	Induction and update	At least annually	Staff/governors

	records		understand responsibilities
AI / new technology	Risk assessments, approvals, DPIA/data-protection checks where required	Before introduction and on review	Safeguarding and governance controls in place
Policy	Statutory changes, incidents, stakeholder feedback	Annually	Policy approved and implemented

17. Related policies

- Child Protection and Safeguarding Policy 2026–27
- ICT and Internet Acceptable Use Policy 2026–27
- Safe Use of Technology – Mobile Phones and Smart Technology Policy 2026–27
- Artificial Intelligence (AI) Policy
- Positive Behaviour and Anti-Bullying Policy 2026–27
- Child-on-Child Abuse Policy 2026–27
- Staff Code of Conduct
- Data Protection Policy and Privacy Notices
- Computing and PSHE/RSE curriculum policies/plans
- Educational Visits and SEND policies.

Appendix 1 – Pupil acceptable use: EYFS and KS1

- I will ask an adult when I would like to use a laptop or iPad.
- I will only use apps and websites that an adult has agreed I can use.
- I know I will always be supervised by an adult when using a laptop or iPad.
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will tell an adult in school if I see something that upsets me on the screen.
- I will not search for or type any inappropriate words.
- I know my teacher can see what I am doing on a laptop or iPad at all times.

Appendix 2 – Pupil acceptable use: KS2

For my own personal safety:

- I understand that my teacher can see what I am doing on a laptop or iPad at all times.
- I know I will be supervised by an adult at all times when using a laptop or iPad.
- I understand that I am only to use apps and websites as agreed by the teacher or adult supervising me.
- I will only communicate online as part of an organised activity.
- I will not bring or use my own personal devices. Any personal devices that are brought to school will be kept in a locked drawer in the school office until the end of the school day.

I will act as I expect others to act toward me:

- I will respect others' work and will not access, copy or delete anyone else's work.

I understand that I am responsible for my actions and conduct, both in and out of school:

- I will remember and follow the online safety rules and apply what I have learnt through e-safety lessons and assemblies, when using technology at home.
- I understand that the school will take action if I am involved in an incident of inappropriate behaviour with others in school or outside of school.

Appendix 3 – Filtering and monitoring annual review record.

Date of review: _____

SLT lead: _____

DSL: _____

IT support/provider: _____

Governor involved: _____

Devices and locations tested:

Filtering tests completed and outcome:

Monitoring arrangements reviewed and outcome:

Generative AI / dynamic content risks considered:

Vulnerable pupil/SEND risk profile considered:

Gaps or concerns identified:

Actions, owners and deadlines:

Date actions checked as complete:

Appendix 4 – Online safety incident recording prompts

- Date/time and people involved
- How concern was identified (disclosure, observation, SENSO/filtering alert, parent report, other)
- Device/platform/service involved
- Nature of concern: content / contact / conduct / commerce
- Immediate safeguarding action taken
- DSL decision and rationale
- Evidence preserved and how (without unnecessary viewing/sharing)
- Parents/carers informed or reason not to inform
- External agency advice/referral
- Behaviour/educational response
- Filtering/monitoring or technical action
- Follow-up, support and learning actions.