



E-Safety Policy for Knypersley First School



The CFLP E-Safety Policy in respect of Knypersley First School has been discussed and adopted by the Local Advisory Board.

Chair of Local Advisory Board:

Miss K Mellor

Responsible Officer:

Headteacher – Miss L Leese

Agreed and ratified by the Local Advisory Board on:

Sept 26

To be reviewed:

Sept 27

Knypersley First School Primary School

(To be used in alongside the Safeguarding Policy/ AI Policy and PSHRE/Computing curriculum documents)

The overall intent of our school curriculum is to:

Recognise uniqueness: in our pupils, staff, resources and whole school community.

Be Inclusive: recognising learning styles, learning needs at all levels and providing solutions to any barriers to learning we encounter.

Engage and Inspire: through knowledge rich, highly enriched, progressive and purposeful contexts.

Promote Aspiration: offering challenge, accountability and responsibility for their learning.

Create citizens of the Future: who thrive on responsibility, see difference as a strength of our community and use democracy to embed their own values and beliefs.

Our E-Safety curriculum strives to drive all of these intentions and links very closely to the achievement and development of them all.

The safety and welfare of our pupils is of the utmost importance. Ensuring that pupils can access technology safely and learn how to participate in the digital world without compromising their safety, privacy or security is an important part of delivering a broad and balanced curriculum.

This policy sets out how the school will respond to online safety and safeguarding concerns arising from pupils' online activity, whether this takes place on or off the school site. It does not create a general duty for the school to monitor pupils' private online activity at home. Where an online issue affects a pupil's safeguarding or welfare, behaviour, staff, other pupils or the wider school community, the school will respond in accordance with its Safeguarding and Child Protection Policy, Behaviour Policy and other relevant school policies.

As Knypersley First School provides education from Reception to Year 4, online safety education will be matched to the age, developmental stage and understanding of our pupils. Children will be taught practical strategies to help them use technology safely, respectfully and responsibly, including protecting personal information, maintaining appropriate privacy, recognising unsafe or inappropriate content and contact, and knowing when and how to seek help from a trusted adult.

This is done by:

- Ensuring that all pupils understand and use the SMART rules in ways that are appropriate to their age and stage of development.
- Helping pupils understand the four areas of online risk identified in Keeping Children Safe in Education 2026: Content, Contact, Conduct and Commerce.
- Supporting pupils to recognise and respond to age-appropriate examples of online risk, including inappropriate content, unsafe contact, unkind or harmful behaviour, scams, advertising and requests for personal information.
- Developing pupils' ability to think critically about information and images they encounter online, including understanding that online content is not always accurate, genuine or suitable.
- Helping pupils understand that photographs, messages and other information shared online may be copied, saved or passed on.
- Ensuring that pupils know how to respond if something online makes them feel worried, uncomfortable or unsafe, including telling a trusted adult.

- Promoting respectful, responsible and safe use of digital technology.
- Implementation

The Computing National Curriculum states that pupils at Key Stage 1 should be taught to:

Use technology safely and respectfully, keeping personal information private; identify where to go for help, support and reporting when they have concerns about content or contact on the internet or other online technologies.

As Knypersley First School provides education from Nursery to Year 4, the school's online safety provision is planned for pupils from Nursery through to the end of Year 4. Teaching will be progressive, age-appropriate and responsive to the needs and experiences of the children.

Online safety is delivered as part of a broad and balanced curriculum and is taught explicitly through Computing and PSHRE, alongside relevant aspects of Relationships Education, health education and personal development. The school will also use assemblies, discussion, stories, scenarios and other appropriate activities to reinforce online safety messages.

The first Computing lesson of each academic year will address the E-Safety Policy and ensure that pupils understand the SMART rules relevant to their age group. Regular differentiated online safety assemblies will also be delivered, using appropriate resources, to foster a culture of safe, respectful and responsible technology use throughout the school.

Pupils will be supported to:

- use the school's digital technology systems, including iPads and computers, safely and responsibly and in accordance with the school's Acceptable Use Agreement;
- understand that personal information should be kept private;
- recognise that information, images and videos found online may not always be accurate, genuine or suitable;
- develop age-appropriate research skills and understand the importance of acknowledging sources and respecting copyright;
- recognise inappropriate, upsetting or harmful content and know how to seek help;
- recognise unsafe or uncomfortable online contact and know that they should tell a trusted adult;
- understand the importance of reporting misuse, bullying, inappropriate content or other online concerns;
- understand that images should not be taken or shared without appropriate permission;
- understand that they should not take, request or share photographs of private areas of the body;
- understand that they should not share personal information, passwords or private details online;
- recognise that people online may not always be who they claim to be;
- understand that online behaviour should be kind, respectful and responsible;
- know how to stop, close, block or report content or contact where this is appropriate and supported by an adult;
- know that they will not be blamed or punished for telling a trusted adult about an online concern; and
- understand that the school's safeguarding procedures may apply to online incidents which affect the welfare or safety of pupils, even when the incident takes place outside school.

The school does not assume that pupils have access to social media or other age-restricted services. Teaching will therefore focus on the underlying skills and behaviours needed to stay safe online, rather than assuming that pupils are using particular platforms or services.

SMART Rules

We expect all pupils within our school/academy to understand the SMART rules for keeping safe both within and outside of school. Our SMART rules (as detailed on childnet.com) are defined as:

S = SAFE

Keep safe by being careful not to give out personal information – such as your name, email, phone number, home address, school name to people who you don't know or trust online.

M = MEET

Meeting someone you have only just been in touch with online can be dangerous. Only do so with your parent's or carer's permission and even then only when they can be present.

A = ACCEPT

Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain nasty messages or viruses.

R = RELIABLE

Someone online might be lying about who they are, and information you find on the internet might not be correct.

T = TELL

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable while using the internet

These are to be introduced gradually from Reception, in the order of:

Tell → Safe → Meet → Accept → Reliable

By following these rules, children should be able to manage most risks posed to them online by understanding when to notify a trusted adult or how to report the risk appropriately e.g. using a service such as <https://www.ceop.police.uk/ceop-reporting/>.

These are to be addressed using the SMART rules as follows:

- Content - Addressed by both the Reliable and Tell rules. This is dependent on whether the content is something that causes concerns/worries for the pupil (in which case Tell is used) or if the content is something that the pupil believes may be untrue they should apply the Reliable rule.
- Contact - Addressed by the Safe, Meet, Accept and Tell rules. This is also linked to the example of online gaming, which is the most common way in which our pupils would make contact with strangers online.
- Conduct – Addressed by the Safe and Meet rules regarding to sharing images and information about themselves and others.
- Commerce – Addressed by both the Safe and Accept rules, as well as targeted specifically by the PSHRE curriculum.

The 4Cs of Online Safety

The school uses the 4Cs framework from Keeping Children Safe in Education to support its understanding of online risks. The 4Cs are Content, Contact, Conduct and Commerce.

The 4Cs provide a framework for staff to identify and respond to online safeguarding risks. Teaching and learning based on the 4Cs will be adapted to the age and developmental stage of pupils and will not introduce children to risks or terminology that are inappropriate for their age.

- **Content** – children may encounter material which is inappropriate, harmful or upsetting. Pupils will be taught to recognise that online content is not always suitable or trustworthy and to tell a trusted adult if they see something that worries or upsets them.
- **Contact** – children may communicate with other people online. Pupils will be taught not to communicate with people they do not know without appropriate safeguards, not to share personal information and to tell a trusted adult if an online interaction makes them uncomfortable or concerned.
- **Conduct** – this relates to how people behave online, including bullying, unkind behaviour and the sharing of information or images without permission. Pupils will be taught to behave respectfully online and to seek help if they or somebody else is being harmed.
- **Commerce** – children may encounter advertising, scams, phishing or attempts to obtain personal or financial information. Pupils will be taught age-appropriate strategies for recognising suspicious messages, advertisements and requests for information and to seek adult help where necessary.

Filtering and Monitoring

As stated by gov.uk, “Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance.”

To address this, we have stringent filtering and monitoring systems in place. Filters are set by our IT specialists EVOLVE IT Support. Furthermore, software is used to monitor all potential threats that are then assessed and addressed on an individual basis by a specially trained member of staff. All concerns about potential issues are then handed to the headteacher and senior leadership team to be addressed appropriately. The E-safety lead is informed on a case-by-case basis to offer specific advice and insights.

Mobile phones and personal devices

The school is a mobile-phone-free environment by default in accordance with the Department for Education’s statutory mobile-phone guidance applying from September 2026. The school’s separate Mobile Phone Policy and arrangements set out the detailed expectations, including any agreed exceptions or reasonable adjustments for individual pupils. The online safety and safeguarding procedures in this policy apply to any mobile phone or personal device used in connection with school

Filtering and monitoring arrangements

The school will maintain appropriate filtering and monitoring systems to support a safe digital environment.

Responsibility for filtering and monitoring will be clearly allocated between the governing body/responsible body, the Headteacher and relevant Senior Leadership Team member, the DSL/DDSL and the school’s IT provider. The school will ensure that:

- filtering and monitoring provision is reviewed for effectiveness at least annually, and following significant changes, new technology, new generative AI tools or a safeguarding incident where relevant;
- checks cover school-managed internet-connected devices and relevant locations, including devices and applications where monitoring is required;
- checks, findings, actions and any identified weaknesses are recorded and followed up;
- monitoring alerts and reports are reviewed promptly and safeguarding concerns are escalated to the DSL/DDSL through the school’s safeguarding procedures;
- the school considers AI-generated, dynamic and personalised content when reviewing filtering and monitoring provision;
- users can be identified where reasonably possible so that safeguarding concerns can be traced and responded to appropriately;
- filtering blocks illegal, inappropriate and harmful content without unreasonably impacting teaching and learning; and
- any weaknesses, failures or inappropriate content identified through filtering or monitoring are reported to the appropriate senior leader, DSL/DDSL and IT provider for action.

The school will maintain records of its annual filtering and monitoring review and any actions arising from it. Filtering

and monitoring arrangements will be considered alongside the school's Data Protection Policy, privacy information and relevant data protection impact assessments.

Impact

The impact of this policy and its enforcement should be that whilst at school, the pupils are:

- demonstrating the age related skills in the Computing Policy for their Year group within the E-Safety area,
- able to access technology, devices and the internet in a way that is safe,
- understand how to apply the SMART rules to their everyday lives.

By time pupils leave the school they are;

- demonstrating the age related skills in the Computing Policy for their Year group within the E-Safety area,
- able to access technology, devices and the internet in a way that is safe, and are able to understand and appropriately use the technology of generations to come,
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations, as well as to identify, differentiate and appropriately respond to/deal with misinformation online/fake news,
- Pupils will develop digital and media literacy skills, including the ability to identify and respond appropriately to misinformation, disinformation, conspiracy theories, AI-generated content and deepfakes. They will be taught to check the source, date, purpose and reliability of information; recognise persuasive, manipulative and commercial content; understand advertising and scams; and consider how algorithms, AI and online platforms can influence what they see and believe.
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so,
- know and understand the reason for policies on the use of mobile and technological devices. They should also know and understand policies/laws on the taking/use of images and on online/cyber-bullying,
- Pupils will understand the safeguarding implications of creating, sharing or receiving images, including AI-generated or digitally altered images and deepfakes. They will understand that the creation, sending, receiving or sharing of nude or semi-nude images is a safeguarding matter and will know how to seek help and report concerns. Relevant incidents will be managed in accordance with the Child Protection/Safeguarding Policy and Behaviour Policy, with mobile-phone and personal-device arrangements applied where relevant.
- understand the importance of adopting good online safety practice when using digital technologies and how to apply the SMART rules to their everyday lives.

Assessment

Children will demonstrate their ability to meet the criteria outlined in the Impact section of this document (above) via:

- Pupil voice,
- During computing and e-safety lessons (recorded using EvidenceMe),
- During relevant PSHRE lessons (recorded using EvidenceMe),

Role of Leaders

Headteacher and Senior Leaders

- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff (see flow chart on dealing with online safety incidents - Appendix 1)

- The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant e.g. National Online Safety.
- The Headteacher and Senior Leaders will ensure that the Online Safety Lead, DSL/DDSL and other relevant staff receive suitable training to enable them to carry out their online safety roles. Staff online-safety updates will be provided at least annually as part of safeguarding updates and will include the school's filtering and monitoring arrangements, relevant roles and responsibilities, how alerts and concerns are escalated, and current and emerging online risks, including AI and AI-generated content.
- The Headteacher and Senior Leaders will receive e-safety concerns via the normal safeguarding channels (e.g. MyConcern) and all e-safety incidents should be treated as a safeguarding concerns.
- Online safety concerns are safeguarding concerns and must be reported through the school's safeguarding procedures to the DSL/DDSL. Concerns should be recorded on the school's safeguarding system where appropriate and escalated in line with the Child Protection/Safeguarding Policy. The DSL/DDSL will determine the appropriate safeguarding response, referral, investigation or other action.
- Liaise with appropriate staff to discuss filters and monitoring, ensure the correct usage and safety of all stakeholders.
- The Headteacher and relevant Senior Leadership Team member will oversee filtering and monitoring arrangements with the DSL/DDSL, the school's IT provider and appropriate governor/LAB oversight. The school will maintain clear roles and responsibilities, conduct and record an effectiveness review at least annually, ensure relevant checks are undertaken, and provide a clear escalation route where weaknesses, inappropriate content or safeguarding concerns are identified.

Online Safety Lead

- Leads the Online Safety Group.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies/documents.
- Coordinates the annual online-safety risk assessment and policy review, ensuring that the policy reflects KCSIE 2026, current online risks, generative AI and AI-generated content, mobile-phone arrangements, filtering and monitoring requirements, and relevant safeguarding, behaviour, acceptable-use and data-protection procedures.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff using relevant courses e.g. National Online Safety.
- Liaises with the MAT and other relevant bodies.
- Liaises with school technical staff (EVOLVE).
- Meets regularly with Online Safety Governor/Director to discuss current issues, review incident logs and filtering/change control logs.
- Attends relevant meetings of Governors/Directors
- Reports regularly to Senior Leadership Team
- Works with the Senior Leadership Team to ensure that parents/carers are provided with appropriate online-safety information and resources, including information about current online risks, age restrictions, privacy and reporting tools, social media and gaming risks, AI and deepfakes, misinformation and disinformation, screen use, and how the school's filtering and monitoring arrangements operate. Parents/carers will also be supported to

understand what pupils are asked to do online in school and, where relevant, who pupils may interact with online.

Teaching and Support Staff

All teaching and support staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school/academy online safety policy and practices
- They have read, understood and signed the staff acceptable use policy/agreement.
- They report any suspected misuse or problem to the DSL/DDSL through the regular safeguarding channels for safeguarding consideration and action in accordance with the Child Protection/Safeguarding Policy. The DSL/DDSL will determine the appropriate response and whether further investigation, referral or other action is required.
- All digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official school systems.

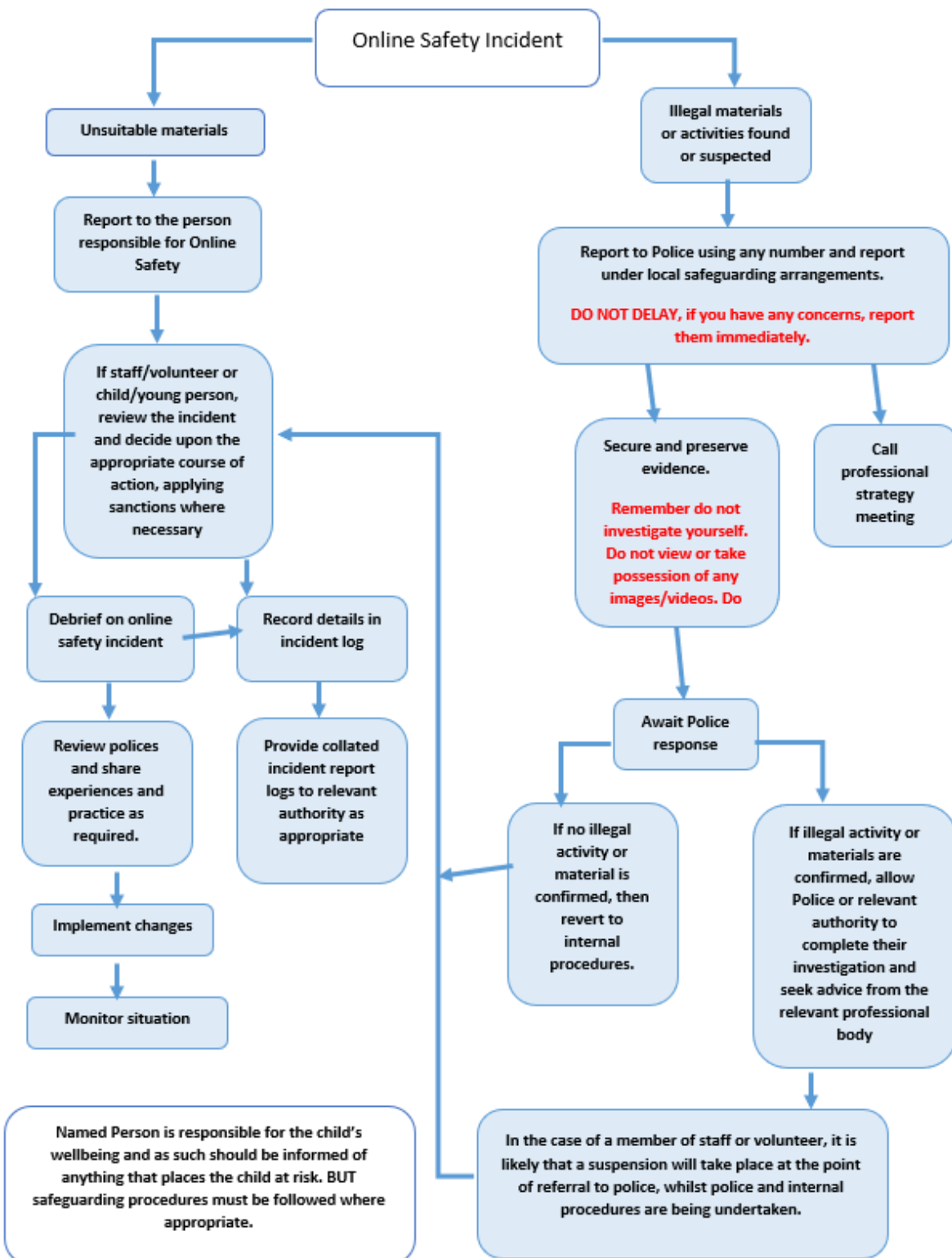
Version	Review Date	Changes Made
V1.0		N/A
V1.1	15/12/22	• Changed review date to January 2024 to ensure 12-month review. • Implementation Section - Now explicitly states that E-Safety is taught as part of a broad and balanced curriculum and links to RE, RSE and HE guidance. • Role of Leaders – Updated to reflect logging on MyConcern and all e-safety incidents being treated as safeguarding incidents. • Online Safety Lead – Updated to reflect responsibility to provide parents with adequate resources to educate themselves about e-safety. • Teaching/Support Staff – Updated to reflect change in reporting procedures to regular safeguarding channels via DSL and DDSL. • Updated reporting channels from paper logs to normal safeguarding channels e.g. MyConcern.

V1.2	26/3/25	• Changes to implementation section to detail the first academic year's computing lesson be about the SMART rules, rather than the first lesson of each term. • Added expectation for fortnightly differentiated assemblies to be delivered using NOS resources in the implementation section. • Added a new section about Filtering and Monitoring to reflect newest guidance. • Added to Headteacher/SLT responsibilities about checking about filtering/monitoring reports.
V1.3	24/09/26	Updated for Keeping Children Safe in Education 2026 and current Department for Education online-safety guidance. Revised the 4Cs to reflect current risks including misinformation, disinformation, conspiracy theories, generative AI and AI-generated content; added a dedicated generative AI section with cross-reference to the school's separate AI Policy; strengthened filtering and monitoring responsibilities, annual review and record-keeping; added mobile-phone/personal-device arrangements; strengthened digital and media literacy, safeguarding response, staff training, parental engagement and staff digital communication requirements; added annual policy monitoring and risk-assessment responsibilities; and updated legislative context and supporting policy cross-references. Highlighted text shows wording added or materially revised in this review

		copy.
--	--	-------

Appendix 1 – Flowchart for Online Safety Incident

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Appendix 2

Online Incident Reporting Log.

[illegible]

External guidance used for this review

- Department for Education – Keeping Children Safe in Education 2026 (in force from 1 September 2026).
- Department for Education – Meeting digital and technology standards in schools and colleges: Filtering and monitoring core standard (updated September 2026).
- Department for Education – Mobile phones in schools (statutory from 29 June 2026; schools expected to follow from September 2026).
- Department for Education – Generative AI: product safety standards (updated January 2026).
- Ofcom – Protection of children duties under the Online Safety Act (updated April 2026).
- Children’s Wellbeing and Schools Act 2026 – Part 3, Online Safety etc., including powers concerning children’s access to specified internet services/features.