E-Safety Policy for

Knypersley First School

2024-25

The CFLP E-Safety Policy in respect of the Children First Learning Partnership has been discussed and adopted by the Local Advisory Board.	
Chair of Local Advisory Board:	*Mrs K Mellor*
Responsible Officer:	*Executive Headteacher – Mrs L Jukes*
Agreed and ratified by the Local Advisory Board on:	*January 2026*
To be reviewed:	

Knypersley First School Primary School

E-Safety Policy 2024

(To be used in alongside the Safeguarding 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.

Intent

The safety and welfare of our pupils and students is of the utmost importance. Ensuring that pupils and students can safely access new technology and learn how to participate in the digital world without compromising their safety and security is a key part of delivering a well-rounded curriculum.

This policy sets out how we will keep pupils/students safe, whether using new technology within the school building or at home.

This is done by:

- Ensuring that all pupils understand and are able to stay safe online by following the SMART rules.
- Ensuring that all children are exposed to, understand and can adhere to the 4Cs mentioned in Keeping Children Safe in Education 2024.
- Making sure that pupils become Outstanding Digital Citizens who are aware of their online actions and the consequences.

Implementation

As stated by the Computing National Curriculum 2013,

Key Stage 1 pupils are expected to;

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

Key Stage 2 pupils are expected to;

> *Use technology safely, respectfully and responsibly; recognize acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.*

This is delivered as part of a broad and balanced curriculum, but also taught explicitly throughout our Computing and PSHRE curriculum (created using RE, RSE and HE curriculum guidance). Each academic year's first Computing lesson requirement is to address the E-safety policy and ensure that all children understand the SMART rules (detailed later) relevant to their age group. Furthermore, regular differentiated E-safety assemblies are taught using National Online Safety resources during fortnightly assemblies to foster a culture of e-safety in our school. However, in the interest of producing outstanding digital citizens, we additionally expect that all pupils:

- are responsible for using the school/academy digital technology systems (e.g. iPads, Computer suites) in accordance with the student/pupil acceptable use agreement (KS1/KS2)
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (KS2)
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so (KS1/KS2)
- will be expected to know and understand the reason for policies on the use of mobile and technological devices. They should also know and understand policies on the taking/use of images and on online/cyber-bullying. (Late KS1 and KS2)
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's/academy's online safety policy covers their actions out of school, if related to their membership of the school. (KS1/KS2)

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/ .

The 4Cs

It is the expectation of class teachers to introduce their class/pupils to strategies to risk assess and deal with content that classified under the 4Cs (as detailed in Keeping Children Safe in Education 2024). The 4Cs are defined as:

- 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.

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.

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 use 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.

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,
- 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,

- 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),
- Through testing to receive their SMART rules wristband.

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 receive e-safety concerns via the normal safeguarding channels (e.g. MyConcern) and all e-safety incidents should be treated as a safeguarding concerns.
- Liaise with appropriate staff to discuss filters and monitoring, ensure the correct usage and safety of all stakeholders.

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.
- 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 are provided with adequate e-safety resources to educate themselves about e-safety.

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 for investigation via the regular safeguarding channels.
- 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	13/03/25	• 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 Head of School/SLT responsibilities about checking about filtering/monitoring reports.

Appendices

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.