E-Safety Policy

Committee ownership for this policy: F&R, C&A, E&C, FGB	FGB
Must be approved by FGB: Y / N	Y
Required by: 1 / 2 • Where 1 is indicated, the requirement is statutory • Where 2 is indicated, the requirement is recommended	1
Frequency of review: annually, bi-annually, every 3 year**s**	Annually
Date last reviewed:	January 2026
Date of next review:	January 2027
Display on website: Y / N	Y
Purpose:	To provide a framework for safe and responsible use of digital technology.
Consultation:	FGB and Staff
Links with other policies:	Keeping Children Safe Policy Acceptable Use Agreements Acceptable Use Policy Behaviour Policy Staff Code of Conduct Data Protection Policy

Introduction

This Online Safety Policy provides a framework for the safe, responsible and purposeful use of digital technology within Kew Riverside Primary School. It recognises that online safety is a fundamental aspect of safeguarding and child protection and is essential to ensuring that children are protected from harm both in school and beyond the school gates.

In accordance with the National Curriculum**,** Keeping Children Safe in Education (KCSIE) 2025, *Teaching Online Safety in Schools*, statutory Relationships, Sex and Health Education (RSHE) guidance, and other relevant statutory and no statutory guidance, the school is committed to safeguarding pupils while developing their digital literacy, resilience and critical thinking skills.

Online safety is embedded within the school's wider safeguarding approach and requires a whole-school, cross curricular response, involving staff, pupils, governors, parents/carers, and external partners. This includes effective filtering and monitoring systems, robust reporting routes, clear expectations for behaviour, and high-quality education that enables pupils to recognise risk, seek help, and behave responsibly online.

As part of this commitment, Kew Riverside Primary School is a smartphone-free school**.** Pupils are not permitted to bring or use smartphones or smart devices on the school site. This approach supports the school's safeguarding responsibilities, reduces potential exposure to online risks, and promotes pupils' wellbeing, focus and positive relationships. In exceptional circumstances, where pupils need to carry a mobile phone for safety reasons (for example, when travelling independently to and from school), the device must be handed in to the school office at the start of the day and collected at the end of the school day, in line with school procedures.

Any online safety concern or incident must always be managed in line with the school's Keeping Children Safe Policy and reporting procedures. Online safety concerns may involve, but are not limited to, exposure to harmful or inappropriate content, online bullying or harassment, sexual exploitation or harmful sexual behaviour, online grooming or coercion, radicalisation or extremism, and risks associated with emerging technologies, including artificial intelligence (AI)**.**

This policy applies to all members of the school community, including staff, pupils, volunteers, governors, parents/carers, visitors and contractors who have access to, or use of, school digital systems. It also applies to the use of personal devices on the school site (where permitted) and to behaviour outside of school where there is a safeguarding concern or impact on the school community.

Pupils are expected to follow the school's Online Safety and Acceptable Use expectations wherever they access the internet**,** whether at home or school, and on any device. Pupils are taught that while the internet offers valuable learning opportunities, it also presents risks, and that responsible behaviour and reporting concerns are essential.

The school uses appropriate filtering and monitoring systems in line with current DfE guidance and is supported in this by its IT provider (Trusol). These systems are designed to reduce the risk of exposure to harmful content; however, no system can be completely effective. Therefore, all users are expected to act responsibly and report concerns immediately.

The school is responsible for ensuring that its digital infrastructure is as safe and secure as reasonably possible and that online safety policies and procedures are implemented consistently. All staff receive regular safeguarding and online safety training and understand that online safety and data protection are everyone's responsibility**.**

Objectives

- To set expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- To equip pupils with the skills and knowledge to use technology safely and effectively and protect from potential online risks.
- Through carefully sequenced and age-appropriate lessons, ensure children recognise when they need help and know how to access it.
- To promote a positive and responsible online culture by all members of the school community: Pupils, staff, governors & parents.
- To ensure reporting routes are embedded and that online safety incidents and outcomes are shared between school leadership and governors as part of the school's online safety awareness raising.
- To ensure parents/carers are informed about current technology and patterns of use.
- To ensure regular and effective training is completed by all staff and governors.
- To comply with legal and regulatory obligations regarding e-safety.

E-Safety Education

Curriculum Integration

- E-safety is integrated into the curriculum through dedicated lessons, embedding it into subjects (PSHE, Computing & RSE), and through regular assemblies and newsletter updates, including anti-bullying week and Safer Internet Day.
- Pupils from Reception to Year 6 will receive age-appropriate instruction about online safety, covering aspects such as cyberbullying (the use of any digital medium to offend, threaten, exclude or deride another person), privacy settings, and the importance of digital footprints ensuring they use technology safely, responsibly, respectfully and securely.
- Pupils from Reception to Year 6 are taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and how to recognise and display respectful behaviour online.
- A Safer Internet Day is held each year to raise awareness for all in the Kew Riverside community and to further build on the sequenced prior learning in the classroom and to ensure that our stance on e-safety stays consistently strong.
- Displays and websites feature resources and details of external organisations such as Childline, Thinkuknow, and CEOP which are provided on our site to give up-to-date information and guidance.
- Children with SEND and those the school perceives as especially vulnerable at any time are given targeted advice and support to help them to use technology.
- In lessons where internet use is pre-planned, it is best practice that Pupils are guided to sites checked as suitable for their use.

Roles and Responsibilities

The School

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to Pupils through:

- Ensuring that personal information is not inappropriately shared.
- Education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- Clear reporting guidance, including responsibilities, procedures, and sanctions. ● Guidance for Pupils, parents/carers

All Staff Responsibilities

School staff are required to sign up to our acceptable use policy as part of their code of conduct. Staff are aware of their responsibilities under PREVENT legislation, which apply to every age group in the school. Staff are expected to:

- Oversee the implementation of the E-Safety Policy and promote an E-Safety culture within the school and participate in training opportunities.
- Staff report any E-Safety incidents (to both DSL and CPOMS for wider stakeholders) and work promptly to resolve them.
- Staff must only use school-related devices and equipment for work-related tasks.
- Confidentiality, professionalism and teachers standards must be maintained at all times.
- Any digital communication between staff and Pupils or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
- All staff should immediately report to a the DSL or DDSL the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

The school permits reasonable and appropriate access to personal social media sites during school hours, however, school staff should ensure that they do not engage in online discussion on personal matters relating to members of the school community.

- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.
- They act as positive role models in their use of social media

When official school social media accounts are established, there should be:

- A process for approval by senior leaders

- Clear processes for the administration, moderation, and monitoring of these accounts - involving at least two members of staff
- Understanding of how incidents may be dealt with under school disciplinary procedures.

Headteacher and Senior Leaders

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding.

- The Headteacher and 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.
- Regularly review the policy and adapt it to changes in legislation and technology.
- The Headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

Governors

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the governor responsible for E-safety; those members will receive regular information about online safety incidents and monitoring. Governors should take part in online safety training/awareness sessions.

Designated Safety Lead (DSL)

The DSL will:

- Hold the lead responsibility for online safety, within their safeguarding role and meet regularly with the online safety governor.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up-to-date capability required to keep children safe whilst they are online.
- Be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- Ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.

Teaching and Support Staff

School staff are responsible for ensuring that:

- They have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices.
- They have read and understood the acceptable use agreement.
- They immediately report any suspected misuse or problem to the DSL for investigation/action, in line with the school safeguarding procedures.
- All digital communications with Pupils and parents/carers are on a professional level and only carried out using official school systems.

- Ensure Pupils understand and follow online safety and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Parental Responsibilities

We believe that by working with families we can help children to manage risk and learn to use technology safely. Listed on our website are details of guidance services and organisations which support parents and carers. We also feature E-Safety advice through school communications such as our newsletter and surveys, and raise its profile through Safer Internet Day.

We expect parents and carers to assist us by monitoring children's access to the internet and to age-appropriate material, and by reinforcing the codes we apply at school.

- We strongly advise parents to follow current age guidelines in the use of social media.
- We strongly recommend that parents install child safety filters on all equipment at home.
- We encourage parents to let us know of any need for information or concerns they may have.
- We encourage parents to regularly talk to their children and to check their online communications.

Pupil Responsibilities

- Pupils will engage in discussions around online etiquette and responsible behaviour.
- Pupils must use technology provided by the school only for educational purposes.
- Personal devices are not allowed in school and will be handed into the office.
- Accessing inappropriate content, cyberbullying, and harassment will not be tolerated.
- Be responsible for using the school digital technology systems in accordance with the Pupil acceptable use agreement.
- Should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Should understand the importance of adopting good online safety practice when using digital technologies both in and out of school.

IT Provider

The IT Provider is responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy and Technical Security Policy to carry out their work effectively in line with school policy.
- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets (as a minimum) the required online safety technical requirements as identified by the DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from local authority and other relevant bodies.

- There is clear, safe, and managed control of user access to networks and devices.
- They keep up-to-date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to DSL & Headteacher for investigation and action.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.

Monitoring systems are implemented and regularly updated as agreed in school policies.

Technology

Mobile Phones

Kew Riverside Primary School is a smartphone-free school. Pupils are not permitted to bring or use smartphones or smart devices on the school site. This approach supports the school's safeguarding responsibilities, reduces potential exposure to online risks, and promotes pupils' wellbeing, focus, and positive relationships.

In exceptional circumstances, which must be agreed in advance with the Headteacher, where a pupil needs to carry a mobile phone, the device must be handed in to the school office at the start of the school day and collected at the end of the day, in line with school procedures.

Social Media & Monitoring

- We do not expect primary age children to have their own account for Facebook (minimum legal age 13) or any other social media/unmonitored messaging services.
- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.
- School use of social media for professional purposes will be checked regularly by a senior leader and the Online Safety Lead to ensure compliance with the social media, data protection, communications, digital image and video policies. In the event of any social media issues that the school is unable to resolve support may be sought from the Professionals Online Safety Helpline.

Filtering & Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours. Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor, in particular when a safeguarding risk is identified.

The school manages access to content across its systems for all users and on all devices using the schools internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre Appropriate filtering.

There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors and regularly reviews all network use across all its devices and services.

  Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead

- All users are aware that the network (and devices) are monitored.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- Physical monitoring (adult supervision in the classroom)
- Internet use is logged, regularly monitored and reviewed

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These may include:

Digital and video images and online publishing

- The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.
- Staff/volunteers must be aware of those Pupils whose images must not be taken/published.
- Those images should only be taken on school devices.
- The personal devices of staff should not be used for such purposes.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act).
- To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other Pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images.
- Care should be taken when sharing digital/video images that Pupils are appropriately dressed.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of Pupils are taken for use in school or published on the school website/social media.

AI Technologies

Staff will only use artificial intelligence (AI) tools with the prior agreement of the Senior Leadership Team (SLT) and solely for the agreed purpose.

To support safeguarding and data protection, staff will only use AI technology that aligns with the Department for Education's *Generative artificial intelligence (AI) in education* guidance and the *Generative AI: Product Safety Standards*.

Our AI guidance is in line with other technologies within the school, DfE policies such as data protection guidelines, technology use in education, and cybersecurity standards.

We expect:

- AI technologies to be used safely, ethically, and effectively within the school environment.
- AI-driven software and hardware to be used solely for educational and administrative applications.

  AI applications not to be used to create or reinforce unfair bias.
- To adhere to GDPR and the UK Data Protection Act 2018, ensuring data used by AI systems is handled securely and confidentially.
- Training for staff is supplied on the safe use of AI technologies and ongoing support mechanisms.
- E-Safety lessons address the use of AI technologies for pupils.

Kew Riverside Primary School recognises that artificial intelligence (AI) can support and enhance pupils' learning. However, it also acknowledges that AI technologies may be misused, including for bullying. This may include the creation or sharing of manipulated content such as "deepfakes" (images, audio, or video that appear real but are artificially generated). Any use of AI to harm, intimidate, or bully others will be addressed in accordance with the school's Anti-Bullying and Behaviour Policies.

Staff should remain vigilant to the potential risks associated with AI tools, particularly as these technologies continue to evolve. Where AI is used by pupils, appropriate supervision and safeguards must be in place to minimise risk and ensure safe, responsible use. Where new AI tools are introduced or used within the school, a risk assessment must be conducted and approved by the Senior Leadership Team prior to implementation.

Reporting and Responding to Incidents

- Any online behaviour that raises safeguarding concerns, including low-level concerns, will be addressed in accordance with the Staff Code of Conduct and the Managing Staff Allegations Policy.
- The school has a responsibility to protect pupil data and how it is stored; any concerns regarding data breaches will be addressed in accordance with the school's Data Protection Policy.
- A clear procedure for reporting E-Safety incidents is established. E-safety concerns should be communicated to our safeguarding lead or to organisations featured on our website.
- All incidents will be investigated promptly, with parents informed of any serious concerns.
- Where there is suspected illegal activity, devices may be checked using the following procedures:
    - One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated device that will not be used by Pupils and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- The taking, sharing or possession of nude and semi-nude images is a safeguarding issue. Staff will respond to and manage any such concerns in accordance with *Keeping Children Safe in Education* and the school's safeguarding policies.
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form

- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- There are support strategies in place e.g. support for those reporting or affected by an online safety incident
- Incidents should be logged on CPOMS
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Learning from the incident (or pattern of incidents) will be provided to stakeholders to ensure updates to policies or education programmes are relevant and to review how effectively the report was dealt with. For staff, this is through regular briefings and for Pupils through assemblies/lessons. Parents/carers are informed through newsletters and our website, while reports are shared with governors, local authority/external agencies through regular safeguarding updates.

Cyber Security

The school recognises that effective cyber security is a key part of safeguarding and is essential to protecting pupils, staff, and personal data when using digital technologies.

The school will take appropriate measures to secure its digital systems, devices, and networks from unauthorised access, misuse, or loss. This includes the use of secure passwords, regular software updates, appropriate access controls, and the secure management of user accounts.

In line with *Keeping Children Safe in Education (2025)*, the school has **appropriate filtering and monitoring systems in place** to help safeguard pupils from harmful or inappropriate online content and to identify potential safeguarding concerns. These systems are designed to:

- block access to inappropriate and harmful content
- monitor activity on school devices and networks
- alert designated staff to potential risks or concerns

The school ensures that:

- filtering and monitoring arrangements are reviewed regularly
- systems are appropriate to the age range of pupils
- roles and responsibilities for managing filtering and monitoring are clearly defined

All staff are responsible for supporting cyber security and online safety by:

- following acceptable use expectations
- keeping passwords and login details secure
- remaining vigilant to cyber risks such as phishing or malicious content
- reporting any concerns related to cyber security, filtering, or monitoring promptly in line with safeguarding procedures

Pupils are taught age-appropriate cyber security and online safety as part of the curriculum, including how to keep personal information safe and how to use technology responsibly.

Any cyber security incidents, filtering or monitoring concerns, or data breaches will be managed in line with the school's Data Protection Policy and safeguarding procedures, and escalated where appropriate.

Recommended Online E-safety Resources

NSPCC

NSPCC – Keeping children safe online

Understanding online safety is challenging for all ages. The NSPCC have advice about how to help you learn about staying safe online as a family, with wider ranging information on the following issues:

- Online safety advice

- Inappropriate and sexual behaviour
- Worried about something online?
- Online safety guides for parents
- Resources for professionals
- Resources for children
- Resources for children with SEND
- Help us keep children safe online

Other Resources

UK Safer Internet Centre: www.saferinternet.org.uk

Child Net: www.childnet.com/parents-and-carers

Internet Matters: www.internetmatters.org/

Parental Controls: www.internetmatters.org/parental-controls/

Monitoring and Reviewing Policy

Kew Riverside recognises the significance of E-Safety as part of its commitment to creating a safe learning environment for all pupils. By adhering to this policy and fulfilling the expectations, we aim to ensure that our pupils are not only digitally competent but also safe and responsible digital citizens.

The governing body of our school is responsible for ensuring that this policy is reviewed regularly and updated in response to technological evolution and statutory guidance.