E-Safety Policy

Date created	November 2024
Review period	Biennial
Next due for review	November 2026
Governors Committee Responsible	FGB
Date Reviewed	November 2024

Our E-Safety Policy has been written by the school, using advice from government guidance and reflects existing legislation, including but not limited to the Education Act 1996, the Education and Inspections Act 2006 and the Equality Act 2010. The template is taken from The Key. Much of the information within the E Safety Policy also links to: Keeping Children Safe in Education Guidance 2024 (KCSiE), the school Behaviour Policy, Anti-Bullying Policy, Child Protection Policy, Safeguarding Policy and Data Protection Policies. It also includes details from the National Curriculum.

Kingsclere CE Primary School E-Safety Policy

1. **Introduction**

This policy outlines the steps the school takes to protect children from harm when using ICT and also how the school proactively encourages children to develop a safe approach to using ICT whether in school or at home. At Kingsclere CE Primary School we are committed to ensuring children learn how to use computers, ICT and modern technologies safely so that they:

- Are able to use ICT safely to support their learning in school
- Know how to use a range of ICT equipment safely in school
- Are able to use ICT and modern technologies outside school in a safe manner, including using ICT as a tool for communication
- Are prepared for the constant changes in the world of technology and understand how to use new and emerging technologies in a safe manner
- Know what to do if they feel unsafe when it comes to using technology and ICT

2. The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- ➢ Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- ➢ Contact – being subjected to harmful online interaction with other users, such as 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, such as 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; and
- ➢ Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

3. Legislation and guidance

This policy is based on the Department for Education’s (DfE’s) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools
Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
Relationships and sex education
Searching, screening and confiscation

It also refers to the DfE’s guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the National Curriculum computing programmes of study.

4. Roles and responsibilities

4.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, staff training, the staff safeguarding newsletter and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Mr Jason Hart.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the Staff Acceptable Use of ICT Policy linked to ICT systems and the internet
- Ensure that online safety is a running and interrelated theme while devising and implementing the whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a ‘one size fits all’ approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

4.2 The headteacher and designated safeguarding lead (DSL)

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

Details of the school’s designated safeguarding lead (DSL) and deputy designated safeguarding leaders (DDSLs) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting staff understanding of this policy and that it is being implemented consistently throughout the school
- Working with the governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place

- Working with the ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

4.3 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

4.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms in the Staff Acceptable Use of ICT Policy regarding ICT systems and the internet and ensuring that pupils follow the E-Safety rules
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting them directly to the DSL. Staff can also access the free Professionals Online Safety Helpline which supports the online safeguarding of both children and professionals. Call 0344 381 4772 or email helpline@saferinternet.org.uk. The helpline is open from Monday to Friday from 10am to 4pm.
- Following the correct procedures by informing the ICT manager to liaise with harrap, if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

4.5 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Support their child in following the E-Safety rules
- Parents/Carers can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

4.6 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the Acceptable Use of ICT Policy.

5. Educating pupils about online safety

5.1 Curriculum Learning

The school will actively teach E-Safety at an age-appropriate level through the curriculum, particularly as part of the Computing, Relationships Sex and Health Education (RSHE) and Personal Social and Health Education curriculum (PSHE) as well as through whole school events such as assemblies and E-safety awareness days.

In **Key Stage 1 (KS1)**, pupils will be taught 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

Pupils in **Key Stage 2 (KS2)** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

5.2 E-Safety Rules (See Appendix 1)

The school's E-safety rules will be on the wall in each classroom and reference will be made to them by staff with children within Computing units, as part of RSHE and PSHE learning and when and where required to emphasise the importance of keeping safe online. The importance of children following our E-Safety rules is outlined in the Home School Agreement.

5.3 Seesaw

The school uses Seesaw to help evidence pupils learning and to support Home Learning. Through interactive lessons, digital portfolios, and two-way communication features, Seesaw keeps everyone in the learning loop by providing continuous visibility into the pupil's learning experience.

Children are also able to use Seesaw at home and school and can use the App to upload videos.

Videos uploaded by children must be:

- Supervised and have the consent of the parent/carer
- Using the templates provided where appropriate
- Only shared on the child's account

Work uploaded by teachers must be:

- Monitored by the Headteacher and Subject Leaders who are second users on all Seesaw accounts
- Adhere to any copyright laws
- Appropriate to the task and age of the pupil

Comments written by children and their parent/carer must be:

- Supervised and have the consent of the parent/carer
- Only shared on the child's account not to a wider group
- Adhere to school rules and expectations about respect for each other

Comments and feedback provided by staff must be:

- Adhering to the school's feedback policy
- Monitored by the Headteacher and Subject Leaders who are second users on all Seesaw accounts
- Timely and relate specifically to the work uploaded by the child
- Only shared on the child's account

Any misuse must be reported immediately to the Headteacher who will respond accordingly. In extreme cases, accounts will be suspended by the school.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5.4 Safe use of Zoom or Teams for the purposes of teaching and learning remotely:

Zoom or Teams may be used as part of remote learning provision. Online safety risks of Zoom and Teams are made aware to staff and mitigated against through following the safe use practices outlined in this policy and in with specific reference to Zoom or Teams as detailed below:

Protection of staff and pupils using Zoom or Teams	Parents/ carers will be expected to be present during a Zoom/Teams meeting Staff and families must be aware of what is in the background of any video calling ensuring that it is appropriate and doesn't compromise GDPR in anyway.

Protection and safe use for staff leading a Zoom/Teams call	For staff, as far as possible, Zoom/Teams meetings will take place from school. Where this is not possible, staff will film in a neutral location such as a living room. Where a Zoom/Teams meeting is used to communicate with one pupil, this will only be carried out when the supervising parent/ carer is visible on the screen and lead by two members of staff.
Protection for children and families being part of a Zoom/Teams call	Zoom/Teams meetings must not be recorded but awareness is shared that as with any live content, this is a safety risk.
Protection of staff and pupils using Zoom/Teams	To ensure safety from uninvited attendees: - All meetings will have a password and waiting rooms to ensure that all invited attendees access the meeting. Parents/Carers must not share meeting details

6. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in newsletters, through Meet the Teacher events or other communications home, and in information via our website or Weduc. This policy will also be shared with parents/carers.

Online safety will also be covered during Meet the Teacher presentations.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

7. Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school Behaviour Policy and Anti-Bullying Policy.)

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training

The school also sends information on cyber-bullying to parents/carers, such as through school newsletters, so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

7.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Behaviour Policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Kingsclere CE Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Kingsclere CE Primary School will treat any use of AI to bully pupils in line with our Behaviour and Anti-Bullying Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment if using new AI tools.

8. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are required to follow the Staff Acceptable Use of ICT Policy. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

More information is set out in the Staff Acceptable Use of ICT Policy.

9. Pupils using mobile devices in school

Pupils may bring mobile devices into school if they walk home independently. No child is permitted to use their mobile phone until walking home at the end of the school day. During the school day, any child that brings a mobile phone to school is required to hand this to their class teacher or cover teacher at the very start of the school day. The teacher will store the phone in a secure locked box throughout the school day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school Behaviour Policy, which may result in the confiscation of their device.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms in the Staff Acceptable Use of ICT Policy.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the headteacher.

11. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour and Anti-Bullying Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Disciplinary Policy and Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, the school safeguarding newsletter and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, threatening, harassing and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in CPOMS.

This policy will be reviewed every year by the headteacher. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

14. Links with other policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy

- Behaviour and Anti-Bullying Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Staff Acceptable use ICT Policy

Appendix 1:

E-Safety Rules (Year R + KS1)

- I will keep my name, password, school or address safe and not share this with anyone online.
- I will only send kind and respectful messages to people.
- I will always log off my computer after using it.
- I will tell an adult if I don't feel comfortable or safe with what I am seeing.
- I will always use the internet with an adult.

Think before you click!

E-Safety Rules (KS2)

- I will log on using my own username and password.
- If I find anything or anyone online that makes me feel uncomfortable, unsafe or uneasy in any way, I will tell an adult immediately.
- I will make sure that all online contact with other children and adults is responsible, polite and sensible.
- I will only upload or add images, video, sounds or text that are appropriate, kind and truthful and will not possibly upset someone.
- I will keep my personal details such as name, phone number or address private when I'm online.
- I know that my behaviour online can be checked, and my parent/ carer contacted if a teacher is concerned.
- I will be responsible for the way I behave online because I know that these rules are to keep me safe.

Think before you click!