Lingfield Primary School

A Personal Best School

E-Safety Policy

Date Agreed by Governors	Spring 2026
Review Date	Spring 2027

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the e-safety of pupils, staff, volunteers and governors
- Deliver an effective approach to e-safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to e-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, anti-Semitism, 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 scam

2. Legislation and guidance

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

- Teaching e-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.

3. Roles and responsibilities

3.1 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 coordinate regular meetings with appropriate staff to discuss e-safety, and monitor e-safety incidents as provided by the designated safeguarding lead (DSL).

The governor who oversees e-safety is Sue Darney.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)
- Ensure that, where necessary, teaching about safeguarding, including e-safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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

3.2 The headteacher

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

3.3 The designated safeguarding lead

Details of the school's DSL Andrew Winter, Deputy DSL: Lucy Longley, Charlotte Bunyan, Anna Sutton, Janice Blatcher are set out in our child protection and safeguarding policy as well as relevant job descriptions.

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

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, ICT manager and other staff, as necessary, to address any e-safety issues or incidents
- Managing all e-safety issues and incidents in line with the school child protection policy
- Ensuring that any e-safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on e-safety

- Liaising with other agencies and/or external services if necessary
- Providing regular reports on e-safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Designated Safeguarding Lead for E-Safety and the Computing Lead

The Designated Safeguarding Lead for E-Safety and the Computing Lead are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any e-safety incidents are logged 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

This list is not intended to be exhaustive.

3.5 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 on acceptable use of the school's ICT systems and the internet , and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any e-safety incidents are logged 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'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents 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 International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect Nobody

3.7 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 terms on acceptable use.

4. Educating pupils about e-safety

Pupils will be taught about e-safety as part of the curriculum:

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, 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** 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

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

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

5. Educating parents about e-safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website, school app and Google Classroom. This policy will also be shared with parents.

If parents have any queries or concerns in relation to e-safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

6. Cyber-bullying

6.1 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 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. Class teachers will discuss cyber-bullying with their classes at an age appropriate level.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

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

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. Acceptable use of the internet in school

All staff and governors are expected to sign an acceptable user agreement regarding the use of the school's ICT systems and the internet as well as the use of personal devices. 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.

More information is set out in the acceptable use agreements in appendix 1.

8. Pupils using mobile devices in school

Pupils may bring mobile devices to school but are not permitted to use them during the school day. Mobile devices will be collected by class teachers at the start of each day and returned just before pupils leave at the end of the day.

The same rules apply during school events such as discos, Year 6 leavers' events and school trips.

9. 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 – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.

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 a member of the Leadership Team.

10. 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 policies on behaviour and ICT and internet acceptable use.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 staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

11. 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 once a year and relevant updates as required (for example through emails, e-bulletins 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, 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 the risks up
- 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 & deputy DSL's will undertake child protection and safeguarding training, which will include e-safety, at least every 2 years. They will also update their knowledge and skills on the subject of e-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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to e-safety on CPOMS.

This policy will be reviewed every year. At every review, the policy will be shared with the governing board.

13. Links with other policies

This e-safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- ICT and internet acceptable use policy

Appendices:

Staff Acceptable Use Agreement - 2025 - Google Docs
EYFS/ KS1 acceptable use agreement (verbal) 2025 - Google Docs
LKS2 acceptable use agreement 2025 - Google Docs
UKS2 acceptable use agreement 2025 - Google Docs

E-Safety Policy - AI Appendix

1. Purpose and scope

This appendix sets out how Lingfield Primary School will use artificial intelligence (AI), including generative AI, in a way that is safe, lawful and educationally beneficial for pupils and staff.

It applies to all members of the school community who use or access AI tools on school systems or for school work, including at home.

2. Principles for AI use

AI will be used to support, not replace, the professional judgement of staff and the wider aims of the curriculum.

Any use of AI is:

- Safe – does not expose pupils to harmful or inappropriate content and complies with safeguarding and filtering/monitoring expectations.
- Lawful – complies with data protection, copyright and exam/assessment regulations.
- Educational – clearly linked to improving teaching, learning or school efficiency, not "technology for its own sake".
- Fair and transparent – avoids unlawful bias and can be explained to pupils, parents, staff and governors.

This policy applies to all AI technologies used within the school, including but not limited to:

- AI systems for assessing student work
- Personalised learning platforms
- Data analysis tools
- Any other AI applications used for educational or administrative purposes

3. Staff use of AI

Staff use approved AI tools to support planning, resource creation, administration and professional development, where this demonstrably reduces workload or improves pupil learning.

Examples of AI use includes:

- Simplifying texts to support lower attainers or children with SEND
- Using learners' sentences/writing to create images for them to evaluate their writing
- Using Reading Progress/Reading Coach to provide individualised feedback or for learners to create their own texts
- Creating specific WAGOLLs
- Creating images for lessons and performances, avoiding copyright issues
- Generating specific questions or word problems in subjects such as maths and science.

Staff at Lingfield Primary School are encouraged to use Microsoft Copilot due to its enhanced privacy and security within the school's Microsoft 365 infrastructure. All use should be linked to their school's Microsoft 365 account/email.

When using any information/data about individuals within the Lingfield Primary School community, staff must use Microsoft Copilot.

Staff can also utilise AI tools embedded within the school's Google system which uses Gemini.

Other generative AI tools (e.g., ChatGPT, Suno, Magic School AI, TeachMate AI) may be used for tasks not involving specific information/data about individuals in the Lingfield Primary School community. Staff should consult with a member of the Leadership Team before using any other generative AI tools not referenced in this policy. If these tools require a login/account, staff should use their school's Microsoft 365 account/email.

Staff will:

- Use only AI tools approved by the school and configured with appropriate safeguards
- Avoid inputting personal data about pupils, parents or staff, or any confidential information, into public AI tools.
- Check AI outputs for accuracy, bias and appropriateness before sharing with pupils or using in decisions.
- Ensure that any AI-generated materials used with pupils meet our standards for quality, accessibility and age-appropriateness.

4. Pupil use of AI

Pupils are introduced to the concept of AI through the PSHE curriculum to build digital literacy and critical thinking.

Where pupil use is permitted, the school will ensure that:

- Use is planned, purposeful and supervised by staff, with clear learning objectives.

- Only age-appropriate, school-approved tools are used, with access controlled according to filtering, monitoring and age-restriction requirements.
- Pupils are taught that AI can be inaccurate, biased and out of date, and that they must cross-check information and never share personal data with AI tools.
- AI is not used to complete assessments in a way that undermines academic honesty or exam regulations

5. Safeguarding, data protection and security

Decisions about introducing new AI tools consider safeguarding, online safety and data protection as set out in KCSIE, UK GDPR and our existing policies. The schools liaises with Judiciam to manage all issues relating to UK GDPR.

Before adoption, leaders will:

- Assess whether the tool meets DfE generative AI product safety expectations and our filtering and monitoring standards.
- Review what data the tool collects, where it is stored, and how it is used, and complete a data protection impact assessment where required.
- Ensure staff receive appropriate training in safe, ethical AI use and understand how to report concerns.

6. Roles and responsibilities

Governing board / trust – approves this appendix and holds leaders to account for safe and effective AI use.

Headteacher and senior leaders – decide which AI tools may be used, ensure compliance with statutory guidance and oversee implementation.

DSL – monitors AI-related safeguarding risks, including harmful content, grooming, cyberbullying and misinformation, and ensures these are reflected in the safeguarding and e-safety framework.

Data protection officer (DPO) – advises on data protection risks and DPIAs for AI tools.

All staff – follow this policy, model safe and ethical AI use, and report concerns or incidents promptly.

Pupils and parents/carers – follow the acceptable use policy and any specific guidance on AI tools and raise concerns with staff where needed.

8. Training, communication and review

The school will provide periodic training for staff on AI opportunities, risks and safe classroom practice, and update this as national guidance develops.

Key messages about safe AI use will be incorporated into the curriculum and shared with parents and carers through existing communication channels.

This appendix will be reviewed at least annually, or sooner if there are significant changes in DfE guidance, technology, safeguarding expectations or local practice.