Name of Policy:	Online Safety Policy
Date first adopted:	November 2025
How often to be reviewed:	November 2027
Reviewed:	
Reviewed:	
Reviewed:	
Reviewed:	
Reviewed:	
Reviewed:	
Reviewed:	
Reviewed:	
Reviewed:	
Reviewed:	
Reviewed By:	LGB

The school is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

In today's digital age, children are increasingly exposed to technology both in and out of school. While digital tools offer immense educational benefits, they also present risks such as cyberbullying, exposure to inappropriate content, online grooming, and data privacy breaches.

At Lulworth and Winfrith Primary school, It is therefore essential for our school to implement robust e-safety and safeguarding measures to protect children and promote responsible digital citizenship.

Our rationale is grounded in the following principles:

- **Child Protection**: Safeguarding children from online harm is a legal and moral responsibility.
- **Education and Empowerment**: Teaching children how to navigate the digital world safely builds resilience and awareness.
- **Staff Responsibility**: All staff must be equipped to identify and respond to e-safety concerns.
- **Partnership with Parents**: Engaging families ensures consistent messaging and support beyond the school environment.
- **Compliance**: Aligning with statutory guidance such as *Keeping Children Safe in Education (KCSIE)* and *UK GDPR* ensures legal compliance.

The purpose of this policy is to:

1. **Define Acceptable Use**: Establish clear expectations for the use of digital devices, internet access, and online platforms by pupils and staff.
2. **Protect Children Online**: Outline procedures to prevent and respond to online risks including cyberbullying, exploitation, and exposure to harmful content.
3. **Guide Staff Practice**: Provide staff with protocols for monitoring, reporting, and managing e-safety incidents.
4. **Promote Digital Literacy**: Support curriculum planning that includes age-appropriate e-safety education.
5. **Ensure Data Security**: Safeguard personal data and ensure responsible use of digital tools in line with data protection laws.
6. **Engage Stakeholders**: Encourage collaboration with parents, carers, and external agencies to reinforce e-safety practices.

Introduction

This policy outlines the approach our school takes to ensure the safety and wellbeing of children when using digital technologies. It supports our statutory duty to safeguard pupils and promotes responsible, respectful, and safe use of technology. KCSIE groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract). These are known as the 4 Cs of online safety.

- Content

Content is anything posted online - it might be words or it could be images and video. Children and young people may see illegal, inappropriate or harmful content when online. This includes

things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

- Contact

Contact is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising. Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

- Conduct

Conduct means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm - for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and viewing or sending pornography.

- Commerce

Commerce is about the risk from things like online gambling, inappropriate advertising, phishing or financial scams. Children and young people may be exposed to these risks directly.

Aims and Objectives

- To protect children from online harm and abuse.
- To educate pupils on safe and responsible use of technology.
- To ensure staff understand their safeguarding responsibilities in digital contexts.
- To promote a whole-school approach to e-safety involving pupils, staff, parents, and governors.

This policy applies to:

- All pupils and staff.
- All devices and platforms used within the school (including school-owned and personal devices).
- All online activity, including email, websites, social media, and educational platforms.

The school Online Safety Lead is Mark Leeming and Tasha Hardy, Deputy Head Teacher, is the Designated Safeguarding Lead.

Our Online Safety Policy has been developed by the school, using government guidance, Project Evolve, CEOP advice and guidance from our PSHE scheme. It has been agreed by the senior management and approved by governors.

The Online Safety Policy and its implementation will be reviewed annually by the staff and governors of the school.

Roles and Responsibilities

Assigning clear roles ensures accountability and coordinated action. It empowers staff, pupils, and parents to take ownership of e-safety and ensures that safeguarding is a shared responsibility supported by leadership and technical expertise.

Headteacher and Designated Safeguarding Lead (DSL)

- Ensure the policy is implemented and reviewed at least every two years.

- Lead on e-safety incidents and concerns (alongside Online Safety Lead)
- Liaise with external agencies when necessary.
- Monitor and respond to filtering reports

Teaching and Support Staff

- Model safe and responsible use of technology.
- Deliver e-safety education as part of the curriculum.
- Report concerns to the DSL promptly and record any concerns on MyConcern

IT Providor (PSD Group)

- Maintain secure systems and filters using SWGfL.
- Monitor usage and flag inappropriate activity which is reported through MyConcern
- Support staff with digital safeguarding tools.

Pupils

- Follow the Acceptable Use Agreement.
- Report anything that makes them feel unsafe online.
- Engage positively with e-safety education.

Parents and Carers

- Support the school's e-safety messages at home, with guidance and support from our weekly newsletters and website.
- Monitor and guide their child's use of technology.
- Report concerns to the school.

Curriculum Integration

E-safety is embedded across the curriculum and is planned strategically throughout the year, to ensure all children cover key skills and develop a progressive understanding of online safety. It is taught through:

- Computing
- PSHE (Jigsaw PSHE scheme)
- Assemblies and themed weeks (e.g. Safer Internet Day, Think you know session, Police Community support services)

Topics include:

- Online bullying
- Privacy and data protection
- Digital footprints
- Reporting concerns
- Online friendships and stranger danger

Acceptable Use Agreements

Acceptable Use Agreements (AUAs) set clear expectations for behaviour for both staff and children when using technology. They help prevent misuse, promote respectful conduct, and provide a reference point for addressing breaches. Age-appropriate agreements also support children's understanding of digital boundaries.

- All staff must sign an Acceptable Use Agreement outlining expectations for safe and respectful use of technology at the start of each academic year.
- Children are taught safe use of technology within school and have posters around school reminding children on these rules.
- These agreements are reviewed annually and adapted for age-appropriateness.

Online Safety Measures

Technical safeguards such as filtering and monitoring are essential to prevent access to harmful content and detect risky behaviour. These measures complement educational efforts and provide a secure digital environment for learning.

- Filtering and monitoring systems from SWGfL are in place to block harmful content, these systems are age and maturity appropriate for our children
- Staff are trained to identify and respond to online safeguarding issues, reporting any issues through MyConcern.
- Devices are regularly updated and secured with the support of our IT provider.
- Pupils are always supervised when using technology.
- The security of the school information systems will be reviewed regularly.
- Virus protection will be updated regularly.
- All digital media is stored securely on Cloud services monitored and maintained by PSD.
- We keep up to date with new technologies, including those relating to mobile phones and handheld devices, and are ready to develop appropriate safety strategies where necessary.
- KS2 pupils are allowed to bring mobile phones into school. However, pupil's mobile phones must be kept in the school office and switched off. Parents must also complete a permission on Arbor and a written permission slip explaining why a phone is needed y their child. The school takes no responsibility for phones which are left in the office. See Mobile Phone Policy.
- Staff mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text, picture or video messages is forbidden.
- It is recommended to staff when on trips that if they have to ring parents from their own personal device they withhold their numbers. However, normal procedures are to contact the school office, who will in turn contact parents.

Social Media and AI Use

Social media and artificial intelligence (AI) are increasingly present in children's lives, both inside and outside the classroom. While these technologies offer opportunities for creativity, collaboration, and learning, they also pose risks such as misinformation, online grooming, data misuse, and exposure to inappropriate content. This section ensures that the school takes a proactive and informed

approach to managing these technologies in a way that safeguards pupils and supports responsible use.

Social Media Use

Policy Statement:

- Pupils are not permitted to access personal social media accounts during school hours.
- Staff must maintain professional boundaries and avoid direct communication with pupils via personal social media platforms.
- The school may use official social media accounts for communication with parents and the wider community, managed by designated staff.
- Any social media content involving pupils (e.g., photos, videos) must have prior parental consent and comply with data protection regulations.

Safeguarding Measures:

- Pupils are taught about the risks of social media, including cyberbullying, privacy breaches, and online grooming.
- Staff monitor pupil discussions and behaviour for signs of social media-related distress.
- The school promotes digital resilience and critical thinking when engaging with online content.

Artificial Intelligence (AI) Use

Policy Statement:

- AI tools may be used in the classroom to enhance learning, provided they are age-appropriate, secure, and aligned with curriculum goals.
- Staff must evaluate AI platforms for safety, data privacy, and educational value before use.
- Pupils must be supervised when interacting with AI tools and taught to question the reliability and accuracy of AI-generated content.

Safeguarding Measures:

- AI tools must not collect or store personal data.
- Staff are trained to understand the ethical implications of AI, including bias, misinformation, and data protection.
- The school ensures transparency in how AI is used and communicates its purpose to parents and carers.

As the technology continues to evolve, so too do the risks that children and young people face online. This can present a challenge for schools. But by using frameworks such as the 4 Cs of online safety, schools and teachers can make sure they have plans and processes that are able to adapt in this ever-changing landscape

Responding to Incidents

Our clear response protocol ensures that e-safety concerns are handled swiftly, sensitively, and effectively. It protects children from further harm, supports victims, and ensures that incidents are documented and addressed in line with safeguarding procedures.

All e-safety concerns must be reported to the DSL. Incidents may include:

- Cyberbullying
- Sexting or sharing inappropriate images
- Online grooming or exploitation

- Exposure to harmful content

The DSL will:

- Record the incident securely on MyConcern
- Take appropriate action (e.g., involve parents, report to authorities).
- Provide support to affected pupils.

Data Protection and Privacy

The school complies with UK GDPR and ensures:

- Personal data is stored securely.
- Pupils' digital work and images are used appropriately.
- Consent is obtained for online platforms and media sharing.

Staff Training

Regular training equips staff with the knowledge and confidence to identify and respond to online risks. It ensures that safeguarding practices remain current and that staff can support pupils effectively in a rapidly evolving digital landscape.

All staff receive annual safeguarding training, including:

- Recognising online risks
- Using school systems safely
- Reporting digital safeguarding concerns

Parental Engagement

Parents/carers play a vital role in reinforcing e-safety messages at home. Engaging them through education and communication builds a consistent approach to digital safeguarding and strengthens the partnership between school and family.

The school provides:

- E-safety workshops provided by our Police Community support team and resources for parents available on our website.
- Guidance on home internet safety and parental controls.
- Regular communication about online trends and risks, through our newsletters.

Policy Review

This policy is reviewed at least every two years by the DSL, Online Safety lead and governing body. Updates are made in response to:

- Changes in legislation
- Emerging technologies
- Feedback from stakeholders