Whitley Park Primary and Nursery School

Online Safety (E-Safety) POLICY

Date of Adoption:	OCTOBER 2025	Date of Review:	Reviewed annually
Author:	NBB	Committee responsible for Review:	FGB
Version:	APPROVED	Date approved:	14.10.2025
CHANGES	UPDATED TO REFLECT KCSIE SEPT 25		

Introduction & Scope

- This policy sets out how Whitley Park Primary and Nursery School seeks to keep pupils, staff, governors, volunteers and visitors safe online (in and out of school).
- It is part of our broader Safeguarding / Child Protection framework; online safety is a core element of safeguarding in our school.
- It refers to and supports obligations under Keeping Children Safe in Education 2025 (KCSIE 2025).
- It covers all digital technology, including school network, WiFi, filtering and monitoring systems; devices (desktop computers, laptops, tablets, mobile devices); virtual learning environments, cloud services, apps, social media, AI tools; remote learning, live streaming, online meetings.
- It applies to all users (pupils, staff, governors, visitors) and all devices whether personally owned or school-provided.

2. Links with KCSIE 2025 and Key Changes

- KCSIE 2025 strengthens and clarifies expectations around online safety:
- Defines online risk into four categories: content, contact, conduct and commerce.
- Explicitly includes misinformation, disinformation and conspiracy theories as safeguarding risks.
- Adds signposting to DfE Generative AI: Product Safety Expectations guidance when considering AI use.
- References cybersecurity standards and resilience to cyber-attack.
- Expects filtering and monitoring systems to be effective, reviewed annually, and detect misuse/bypass attempts.
- This policy will be reviewed annually or sooner if guidance/technology changes.

3. Roles & Responsibilities

- Governing Body: Ensure robust policy, monitoring, training and resources.
- Headteacher: Oversee implementation, training and reporting.
- DSL: Investigate incidents, oversee safeguarding records, support staff.
- IT support: Maintain filtering/monitoring, cybersecurity and technical support.
- All Staff: Model safe practice, follow policy, report concerns.
- Pupils: Follow rules, report concerns, engage with curriculum.
- Parents/Carers: Support safe practice at home, follow Acceptable Use Policy.

4. Acceptable Use & Digital Behaviour Standards

- All users must sign an Acceptable Use Policy (AUP).
- Staff communicate with pupils only via approved platforms.
- Personal devices/BYOD must comply with filtering/monitoring rules.
- Staff/pupils must follow social media guidelines; official accounts centrally managed.
- AI tools used in line with DfE expectations; training provided on risks and responsible use.

5. Filtering, Monitoring & Technical Safeguards

- Industry-standard (Securly) filtering and monitoring systems are in place and regularly reviewed with the IT support provider (Softegg)
- Cybersecurity includes firewalls, antivirus, intrusion detection, backups and access control.
- Devices are managed to limit unapproved software and enforce updates.
- Annual audit of filtering/monitoring effectiveness conducted by DSL and IT Support contractor.

6. Education, Training & Awareness

- Pupils receive age-appropriate online safety education as part of the PSHE curriculum
- Staff (and governors) receive induction and regular updates on online safety risks.
- Parents/carers are provided with workshops and guidance to support safe practice at home.

7. Responding to Online Safety Incidents & Logging

- All incidents are reported to DSL and logged securely.
- Illegal content is reported to law enforcement; harmful but not illegal content managed proportionately.
- Sanctions for misuse follow school behaviour/suspension and exclusion policies.
- Serious incidents are reported to governors and external bodies if required.

8. Rights, Privacy & Data Protection

- All data handling complies with UK GDPR and Data Protection Act.
- Users are informed their activity may be monitored and logged.
- Users have rights to access or request deletion of personal data (where lawful).

9. Review, Monitoring & Continuous Improvement

- Policy reviewed annually or after significant change.
- DSL, IT Lead, SLT and governors monitor implementation and incidents.
- Stakeholder feedback informs improvements.

10. Appendices

- Appendix A: Acceptable Use Agreement (Staff)
- Appendix B: Acceptable Use Agreement (Pupils)
- Appendix C: Parental / Carer Consent Form
- Appendix D: Glossary of Terms
- Appendix E: Useful Resources & Links

Appendix A: Acceptable Use Agreement (Staff)

As a member of staff, I agree to:

• Use school devices, internet and systems for professional/educational purposes only.

• Keep passwords secure and not share login details.

• Communicate with pupils only through approved school platforms.

• Not access, create or share inappropriate content.

• Report any online safety concerns to the DSL immediately.

• Follow the school's safeguarding and data protection policies.

Signed: _____ Date: ____ / ____ / 20____

Appendix B: Acceptable Use Agreement (Pupils)

As a pupil at [School Name], I agree to:

• Use school devices and the internet safely and responsibly.

• Never share personal information online without permission.

• Be kind and respectful when communicating online.

• Not try to access inappropriate or blocked content.

• Tell an adult or teacher if I see something that worries me.

Signed (Pupil): _____ Date: ____ / ____ / 20____

Signed (Parent/Carer): _____ Date: ____ / ____ / 20____

Appendix C: Parental / Carer Consent Form

I have read and discussed the school's Online Safety Policy and Acceptable Use Agreement with my child.

I understand that my child must follow the rules to ensure their safety and the safety of others online.

I give permission for my child to use school digital systems and online platforms under supervision.

Child's Name: _____

Parent/Carer Name: _____

Signature: _____ Date: ____ / ____ / 20____

Appendix D: Glossary of Terms

• AUP – Acceptable Use Policy

• DSL – Designated Safeguarding Lead

• Filtering – Technology that blocks access to harmful/inappropriate content.

• Monitoring – Technology that logs and alerts staff to unsafe or risky activity.

• AI – Artificial Intelligence; tools that generate or process content.

• GDPR – General Data Protection Regulation (UK version).

Appendix E: Useful Resources & Links

• UK Safer Internet Centre – https://saferinternet.org.uk

• CEOP (Child Exploitation and Online Protection) – https://www.ceop.police.uk

• NSPCC Online Safety – https://www.nspcc.org.uk/keeping-children-safe/online-safety

• Keeping Children Safe in Education (KCSIE) 2025 – DfE

• DfE Guidance on Generative AI – https://www.gov.uk

• National Cyber Security Centre (NCSC) – https://www.ncsc.gov.uk