Wolsey House Primary School

Online Safety Policy

Policy date: October 2026

Policy review date: October 2027

Together we grow, achieve and thrive.

1. Purpose, scope and aims

Online safety is an essential part of safeguarding. Wolsey House Primary School will protect and educate pupils, staff and the wider school community in their use of technology and maintain clear arrangements for identifying, reporting, responding to and learning from concerns.

This policy applies to governors, employees, agency staff, volunteers, contractors, visitors, pupils, parents and community users when they use school systems or devices. It also applies to personal technology used on the school site and to online activity outside school where it affects a pupil, member of staff or the safe and orderly operation of the school.

The school aims to:

- provide a safe digital environment without unreasonably restricting teaching and learning;
- identify and support pupils who may be at greater risk online, including pupils with SEND or communication needs;
- teach pupils to use technology safely, respectfully, critically and responsibly;
- maintain effective filtering, monitoring, cyber security and access controls;
- ensure concerns are reported, recorded on CPOMS where appropriate, assessed and escalated promptly; and
- work constructively with parents, carers, external agencies and service providers.

2. The four areas of online risk

The school plans its approach around the four overlapping categories used in Keeping Children Safe in Education:

- **Content:** exposure to illegal, inappropriate or harmful material, including pornography, racism, misogyny, antisemitism, self-harm or suicide content, violence, radicalisation, extremism, misinformation, disinformation, conspiracy theories and AI-generated or manipulated content.
- **Contact:** harmful interaction with other users or AI applications that simulate interaction, including peer pressure, commercial targeting, grooming, exploitation, coercion, extortion and adults or children misrepresenting their identity.
- **Conduct:** behaviour that causes or increases harm, including online bullying, abusive or discriminatory messages, impersonation, doxxing, the consensual or non-consensual sharing of nude or semi-nude images, sexual harassment and the creation or sharing of AI-generated sexualised images.
- **Commerce:** gambling, inappropriate advertising, scams, phishing, in-app purchases, financial exploitation and other commercial risks.

3. Legal and guidance framework

This policy has regard to current legislation and guidance, including:

- Keeping children safe in education 2026
- Relationships education, relationships and sex education and health education statutory guidance
- Teaching online safety in schools
- Filtering and monitoring core standard
- Cyber security core standard
- Searching, screening and confiscation

- Mobile phones in schools
- Prevent duty guidance
- Sharing nudes and semi-nudes guidance for education settings
- Generative artificial intelligence in education

Relevant legislation includes the Education Acts 1996, 2002, 2011 and the Education and Inspections Act 2006; Children Acts 1989 and 2004; Equality Act 2010; Data Protection Act 2018 and UK GDPR; Data (Use and Access) Act 2025; Computer Misuse Act 1990; Protection from Harassment Act 1997; Sexual Offences Act 2003; Voyeurism (Offences) Act 2019; Online Safety Act 2023; and copyright and communications legislation.

4. Roles and responsibilities

4.1 Governing Body

- approves this policy and holds the Headteacher to account for consistent implementation;
- ensures online safety is a running and interrelated theme within safeguarding, curriculum, staff training and parental engagement;
- ensures appropriate filtering and monitoring systems are in place and receives assurance about their effectiveness;
- ensures the effectiveness of filtering and monitoring is formally reviewed and recorded at least once in every academic year;
- receives anonymised information about incidents, trends, training, risks and actions at least annually; and
- ensures governors receive appropriate safeguarding, online safety and cyber-security training.

4.2 Headteacher and senior leaders

- promote a culture in which online safety concerns are recognised and reported;
- ensure this policy, acceptable-use arrangements and related procedures are implemented;
- allocate resources, training and suitable cover for key safeguarding responsibilities;
- approve changes to filtering, monitoring, technology and online services following appropriate consultation;
- ensure serious incidents, staff concerns and cyber incidents follow the correct safeguarding procedures; and
- work with the DSL, Online Safety Lead, IT provider, Data Protection Officer and governors.

4.3 Designated Safeguarding Lead

- holds lead responsibility for online safety within the safeguarding role;
- understands the school's filtering and monitoring systems and processes;
- receives, assesses and coordinates the response to safeguarding concerns, including concerns generated by monitoring systems;
- ensures safeguarding incidents and decisions are recorded accurately on CPOMS;
- liaises with children's social care, police, Prevent, CEOP and other agencies where necessary;
- leads the annual online-safety risk assessment and contributes to the annual filtering and monitoring review; and
- reports anonymised themes and assurance information to senior leaders and governors.

4.4 Online Safety Lead

- works closely with the DSL and curriculum leaders;

- coordinates policy review, curriculum mapping and awareness raising;
- provides or identifies staff, pupil and parent guidance and training;
- monitors emerging risks and uses incidents and pupil voice to inform provision; and
- supports regular parent communication, including the school's online-safety newsletters.

4.5 IT technical support

- maintains secure, appropriately configured networks, accounts, devices, backups, filtering and monitoring systems;
- provides reports and timely support to the DSL and senior leaders;
- completes and records checks, maintenance and actions arising from reviews;
- applies the principle of least privilege, timely software updates and suitable authentication;
- does not make safeguarding decisions in isolation; and
- reports system failures, suspicious activity, data incidents and cyber incidents immediately through agreed routes.

4.6 All staff, volunteers and contractors

- read and follow this policy, the Staff Code of Conduct and the applicable acceptable-use agreement;
- understand their role in filtering and monitoring and how to report a concern or system failure;
- supervise pupils' use of technology and use school-approved systems and communication channels;
- report safeguarding concerns to the DSL without delay and record them on CPOMS as required;
- do not investigate, search for, copy or forward illegal or sexual imagery;
- model safe, respectful and professional online behaviour; and
- use artificial intelligence only in accordance with the school's AI Policy.

4.7 Pupils, parents and visitors

Pupils will follow the age-appropriate acceptable-use agreement, report anything worrying and use only authorised systems. Parents and carers are expected to support the school's rules, raise concerns promptly and help their child use personal devices safely. Visitors and community users must follow staff instructions and the relevant acceptable-use conditions.

5. Online safety education

Online safety will be taught through computing, relationships and health education, English and the wider curriculum. It will be revisited regularly and adapted to pupils' age, development, SEND, communication needs, experiences and the risks affecting the school community. Teaching will avoid victim-blaming and will make clear that a child who seeks help will be supported.

Pupils will learn, at an age-appropriate level, to:

- use technology safely, respectfully and responsibly and recognise acceptable and unacceptable behaviour;
- protect personal information, passwords, privacy, location and online identity;
- recognise harmful content, contact, conduct and commercial pressure and know how to block, report and seek help;
- understand that people may misrepresent themselves and that online relationships can involve grooming, coercion or exploitation;

- evaluate information and recognise misinformation, disinformation, manipulated media, deepfakes and AI-generated content;
- understand consent, boundaries, online bullying, sexual harassment and the risks of sharing images;
- understand that online material may be copied and redistributed and can be difficult to remove;
- respect copyright, authorship and other people's work; and
- manage screen time, online conflict, persuasive design and the effect of technology on wellbeing.

The curriculum will draw on National Curriculum computing requirements, the statutory Relationships and Health Education guidance effective from September 2026, National Online Safety resources and relevant national initiatives such as Safer Internet Day and Anti-Bullying Week.

6. Supporting pupils who may be more vulnerable

A single approach will not meet every child's needs. Teaching, supervision, reporting routes and consequences will be adapted where necessary for pupils with SEND, speech and language needs, EAL, mental-health needs, prior experiences of abuse or other vulnerabilities. Staff will consider whether apparently risky behaviour reflects exploitation, unmet need, developmental understanding or a safeguarding concern. Reasonable adjustments will not remove the child's right to protection or lower expectations that harmful behaviour must stop.

7. Working with parents and carers

The school will publish this policy, share age-appropriate acceptable-use expectations and provide regular information through newsletters, the website, meetings and targeted communication. Advice will cover emerging applications, social media age limits, gaming, privacy and parental controls, scams, sharing images, cyberbullying and routes for help. Parents will be contacted following incidents where appropriate, unless doing so would increase risk or conflict with advice from police or children's social care.

8. Acceptable use and supervision

School technology is provided primarily for education, safeguarding and legitimate school business. Users must have an authorised account, keep credentials secure, access only information they are entitled to use and follow copyright, data-protection and records-management requirements.

- Pupils will use online services under the level of supervision appropriate to their age, needs and the activity.
- Teachers will check or select suitable resources and provide a clear learning purpose.
- Users must not bypass filtering or monitoring, install unauthorised software, connect unauthorised equipment, access another person's account, or create or distribute illegal, abusive, discriminatory, sexual or harmful material.
- Official school systems must be used for communication with pupils and parents. Personal email, messaging accounts and social-media accounts must not be used.
- School images and recordings may be made, stored and published only through approved devices, services and permissions.
- Generative AI may be used only through approved tools and for approved purposes under the AI Policy.

9. Personal devices, mobile phones and smart technology

The school's Mobile Phone Policy sets the detailed arrangements. Personal phones and connected devices brought by pupils must be switched off and stored as directed throughout the school day unless an individual exception has been agreed for medical, safeguarding, SEND or other exceptional reasons. Smart watches must not be used to communicate, record, photograph or access online services during the school day.

Staff must follow the Staff Code of Conduct when using personal devices. Personal devices must not be used to photograph or record pupils, store school information or communicate with pupils or families. Any authorised exception must be explicit and securely managed.

10. Filtering and monitoring

The school will maintain filtering and monitoring arrangements that are proportionate to the age and needs of pupils, the school's risk profile and its use of technology, including generative AI. Filtering will block harmful and inappropriate content without unreasonably affecting teaching and learning. Monitoring will help identify activity that may indicate risk and will be supported by timely human review and safeguarding action.

Roles are allocated as follows: senior leaders govern the provision and document decisions; the DSL understands the systems and leads safeguarding responses; the IT provider maintains the technical controls and reports; staff remain alert, supervise use and report concerns; governors receive assurance.

At least once every academic year, the school will complete and record a review of effectiveness. This will include checks that filtering works appropriately on all internet-connected devices in all relevant locations; consideration of pupils' age, SEND, EAL and risk profile; analysis of incidents and monitoring reports; review of what is blocked or allowed; and actions, owners and completion dates. Material changes and serious incidents will trigger an earlier review.

Filtering changes must follow an authorised process. A member of staff who believes legitimate educational content is blocked, or that harmful content is accessible, must report this through the school's agreed IT reporting route and inform the DSL where there is a safeguarding concern. Staff must not attempt to bypass controls.

11. Cyber security and data protection

The school will work towards and maintain the DfE cyber-security core standard. Controls will include named leadership, risk assessment, asset and account management, least-privilege access, multi-factor authentication where appropriate, secure configuration, updates and patching, malware protection, tested backups, incident planning and staff awareness.

- Suspicious emails, unexpected authentication prompts, lost devices, unauthorised access, malware and suspected data loss must be reported immediately.
- Users must not approve unexpected multi-factor authentication requests, disclose passwords or connect unknown storage devices.
- Personal data will be handled in accordance with the Data Protection Policy and privacy notices.
- A cyber incident that may involve personal data, safeguarding or loss of service will be escalated to the Headteacher, DSL, DPO and IT provider as applicable. External reporting will be completed where required.

12. Online bullying, child-on-child abuse and harmful sexual behaviour

Online bullying and abuse will be taken as seriously as behaviour occurring face to face. Staff must not dismiss conduct as banter, part of growing up or an inevitable feature of online life. Concerns may involve abusive or misogynistic messages, group-chat exclusion, harassment, threats, impersonation, image-based abuse, coercion, sexual harassment, stalking or the use of AI to alter or create harmful material.

The school will protect and support the child who may have experienced harm, assess the needs and risk presented by the child alleged to have caused harm, consider other affected children and take proportionate safeguarding and behaviour action. Restorative work will take place only where safe, appropriate and freely agreed; it will never be required as a condition of support.

13. Nude and semi-nude images, deepfakes and illegal content

A concern involving a nude or semi-nude image of a child—including an AI-generated or digitally altered image—must be reported to the DSL immediately. Staff must not view, copy, print, forward, download or ask a child to share the image. The DSL will follow UKCIS guidance, assess immediate risk, preserve relevant information without unnecessarily viewing content and seek advice from police, children's social care or specialist services where appropriate.

If illegal content is suspected, staff must not conduct their own investigation or use a search engine to look for similar material. The school will follow safeguarding and evidence-preservation advice and may report to CEOP, the Internet Watch Foundation, police or other relevant bodies.

14. Searching, confiscation and examination of devices

Only the Headteacher or an authorised member of staff may search a pupil or examine data or files on a device, and only in accordance with current statutory guidance and the school's Searching, Screening and Confiscation arrangements. Decisions will consider safeguarding, proportionality, the pupil's age and SEND, the reason for the search, the need for another member of staff to be present and whether police advice is required.

Staff must never intentionally view suspected child sexual abuse material. Where such material may be present, the device should be secured without searching further and the DSL should obtain specialist advice.

15. Reporting and responding to concerns

A pupil may report to any member of staff verbally, in writing, through drawing or through the school's established worry or check-in arrangements. Reasonable adjustments will be made so pupils with SEND or communication needs can report safely.

Staff will:

- listen calmly, reassure the child and avoid blame;
- not promise confidentiality;
- ask only enough open questions to establish immediate safety;
- report a safeguarding concern to the DSL or deputy without delay;
- make an accurate, factual and timely record on CPOMS;
- preserve relevant usernames, URLs, dates, times and messages without forwarding illegal or sexual imagery; and
- take emergency action or contact police where there is immediate danger.

The DSL will assess safety, wishes and needs; consider the four areas of risk, context, repetition, power imbalance and potential criminality; decide whether school action, early help, children's social care, police, Prevent, health or specialist advice is required; and ensure support, risk management, communication and review. A decision not to refer externally will be recorded with reasons.

16. Staff conduct and allegations

A concern about a member of staff's online conduct, communication or use of technology must be reported to the Headteacher. A concern about the Headteacher must be reported to the Chair of Governors. The school will follow the Managing Allegations, Low-Level Concerns, Staff Code of Conduct and Whistleblowing procedures and consult the Local Authority Designated Officer where the threshold may be met.

17. Training

All staff will receive online-safety and filtering-and-monitoring training at induction, within safeguarding training and through updates at least annually and when risks or systems change. Training will include reporting routes, online abuse, child-on-child harm, radicalisation, scams, misinformation, AI and deepfakes, image-based abuse, cyber security and data protection. The DSL and deputies will maintain current specialist knowledge. Governors and volunteers will receive training proportionate to their roles.

18. Recording, monitoring and review

Safeguarding incidents will be recorded on CPOMS using appropriate categories and linked pupils. Technical faults and cyber incidents will also be recorded through the relevant IT or data-breach route. Records will distinguish observed facts, the child's own words, professional assessment, decisions, actions and outcomes.

The DSL and Online Safety Lead will analyse anonymised themes, repeat concerns, locations, platforms, protected characteristics, SEND, vulnerabilities and the effectiveness of interventions. The Governing Body will receive assurance information at least annually without unnecessary personal information.

This policy, the school's online-safety risk assessment and the effectiveness of filtering and monitoring will be reviewed at least once every academic year and sooner after significant guidance changes, new technology, a serious incident or evidence that controls are not working.

19. Related policies

This policy should be read with the Safeguarding and Child Protection Policy; Child-on-Child Abuse Policy; Behaviour and Anti-Bullying policies; Staff Code of Conduct; Data Protection Policy and Personal Data Breach Procedure; Artificial Intelligence Policy; Mobile Phone Policy; Prevent Risk Assessment; Searching, Screening and Confiscation arrangements; Acceptable Use Agreements; Complaints Policy; Whistleblowing Policy; and relevant curriculum policies.

Appendix 1 EYFS and Key Stage 1 acceptable use agreement

My safe technology promises:

- I will ask an adult before I use a school computer, tablet, website or AI tool.
- I will use only the apps and websites my teacher tells me to use.
- I will keep my password private.
- I will be kind and respectful when I use technology.
- I will not share my name, address, photograph or other personal information without an adult's permission.
- If I see or hear something that worries, upsets or confuses me, I will stop and tell a trusted adult. I will not be in trouble for asking for help.
- I will look after school equipment and tell an adult if something is broken or not working.
- I understand that school systems are checked to help keep everyone safe.

Pupil name	
Pupil signature or mark	
Parent or carer signature	
Date	

Appendix 2 Key Stage 2 acceptable use agreement

When I use school technology or online services, I will:

- use them for learning and only with permission;
- use only my own account and keep my password private;
- protect personal information, privacy and location;
- communicate kindly and never bully, threaten, exclude, impersonate or embarrass someone;
- tell a trusted adult immediately if I see, receive or do something that worries me;
- not open unexpected links or attachments, arrange to meet an online contact, or respond to suspicious requests;
- not create, search for, save or share sexual, violent, hateful or otherwise harmful content;
- use AI only when a teacher has approved the tool and task, and be honest about how it helped;
- not bypass security, filtering or monitoring or install anything without permission;
- respect copyright and other people's work;
- keep any personal phone or connected device switched off and stored as directed; and
- understand that school systems are monitored to keep people and information safe.

I understand that staff will help me if I report a concern. If I misuse technology, the school will respond under its safeguarding and behaviour procedures and will take account of my age, needs, intent and the impact on others.

Pupil name	
Pupil signature	
Parent or carer signature	
Date	

Appendix 3 Adult acceptable use agreement

This agreement applies to staff, governors, volunteers, contractors and visitors who use school systems or information. I will:

- use school technology only for authorised purposes and follow relevant policies;
- use my own authorised account, strong credentials and multi-factor authentication where provided;
- keep devices secure, lock the screen when unattended and report loss or suspected compromise immediately;
- use official school systems for professional communication;
- access, use and share only the information required for my role;
- report safeguarding concerns to the DSL and record on CPOMS as required;
- report filtering failures, harmful content, suspicious messages, cyber incidents and data breaches promptly;
- supervise pupils appropriately and model safe professional behaviour;
- use AI only as permitted by the AI Policy and never put personal, safeguarding or confidential information into an unapproved service; and
- respect copyright, confidentiality, privacy, records-management and data-protection requirements.

I will not:

- share credentials, use another person's account or allow unauthorised access;
- bypass filtering, monitoring or other security controls;
- install unauthorised software or connect unauthorised equipment;
- use personal devices to photograph pupils, store school information or communicate with pupils or families;
- access, create, save or share illegal, sexual, discriminatory, abusive or harmful content; or
- use school systems for private business, political campaigning or activity that may bring the school into disrepute.

Name	
Role	
Signature	
Date	

Appendix 4 Staff response guide

If a pupil reports or staff discover an online-safety concern:

Stage	What to do	Important limits
1. Make safe	Address immediate danger, provide reassurance and contact emergency services if required.	Do not blame the child or promise confidentiality.
2. Report	Contact the DSL or deputy without delay.	Do not wait until the end of the day for a safeguarding concern.
3. Record	Make a factual CPOMS record using the child's own words where relevant.	Separate fact, professional assessment and action.
4. Preserve	Record usernames, URLs, dates and times and keep the device secure if advised.	Do not copy, forward, download or unnecessarily view sexual or illegal imagery.
5. Follow direction	The DSL decides referrals, parent contact, risk management, support and review.	Do not investigate or question children repeatedly.

Appendix 5 Annual online safety review record

Complete at least once each academic year and after a serious incident or material system change. Retain supporting evidence and report key findings to governors.

Review area	Evidence and finding	Action, owner and deadline	Completed / reviewed
Online-safety risk assessment reflects current pupils, technology and incidents			
Filtering tested on all internet-connected device types and relevant locations			
Monitoring alerts, reports and safeguarding responses reviewed			
Roles, escalation routes and service-provider contacts confirmed			
Blocks, allow lists and educational impact reviewed			
SEND, EAL, age and vulnerability considered			
Cyber-security controls, accounts, backups and incident plan reviewed			
Staff, governor, pupil and parent training and communication evaluated			
AI tools and AI-related risks considered			
Policy, acceptable-use agreements and linked procedures updated			

Review led by: _____ Date: _____

DSL: _____ IT provider: _____

Governor assurance reported on: _____ Next review due: _____