Online Safety Policy

Wallands Community Primary and Nursery School

This policy was adopted on 1/9/26

This policy is due for review on 31/8/27

Contents

Policy at a glance 4

Five things every member of staff should remember 4

Where to go for more detail 4

If you are unsure what to do 4

1. Policy purpose and aims 5

2. Scope and application 6

3. Online safety principles and whole-setting approach 7

4. Roles, leadership and accountability 8

5. Education, curriculum and digital resilience 9

6. Vulnerable children and learners 10

7. Staff awareness, training and professional expectations 11

8. Working with parents and carers 12

9. Reporting and responding to online safety concerns 13

10. Filtering, monitoring and access to technology 14

11. Cyber security and account security 15

12. Artificial intelligence and emerging technology 16

13. Communications, social media and image use 17

14. Mobile phones, personal devices and wearable technology 18

15. Data protection, privacy and information sharing 19

16. Community use, third-party providers and external access 20

17. Monitoring, assurance and review 20

18. Related policies, procedures and supporting documents 21

Policy at a glance

Online safety is part of safeguarding. Everyone has a role in preventing harm, using technology responsibly and reporting concerns promptly.

Five things every member of staff should remember

1. Only use approved systems and maintain professional boundaries.
2. Supervise technology appropriately and remain professionally curious.
3. Report online safety and safeguarding concerns promptly to the DSL or safeguarding team.
4. Do not investigate illegal or sexual imagery yourself.
5. Follow the linked standards and procedures for filtering and monitoring, cyber security, AI, communications and personal devices.

Where to go for more detail

This core policy sets the organisation's principles and accountability. Operational detail sits in the following documents:

- Incident Response Procedure
- Filtering and Monitoring Standard and Annual Assurance Checklist
- Cyber Security and Account Management Standard
- AI and Emerging Technology Procedure
- Communications, Social Media and Image Use Procedure
- Mobile Phone and Personal Device Policy
- Staff Online Safety Quick Guide
- Local Safeguarding Contacts and Referral Schedule

If you are unsure what to do

Prioritise safety, preserve relevant information where it is safe and lawful to do so, avoid unnecessary investigation, and seek advice from the DSL or safeguarding

team. Where there is a significant or immediate risk of harm then appropriate action must be taken without delay.

1. Policy purpose and aims

Online safety is an integral part of safeguarding. Digital technology creates significant opportunities for teaching, learning, communication, participation and access to support, but it can also expose children and adults to harm. This policy sets out the setting's strategic approach to preventing online harm, promoting safe and responsible use of technology, and responding effectively when concerns arise.

The aims of this policy are to:

- safeguard and promote the welfare of children and learners when they use technology, online services and connected devices;
- support a whole-setting culture in which online safety is understood as part of safeguarding, behaviour, curriculum, staff conduct, data protection and digital governance;
- ensure that leaders, governors or proprietors, the Designated Safeguarding Lead (DSL), staff and technical providers understand their respective responsibilities;
- provide children and learners with age-appropriate knowledge, skills and confidence to recognise risk, make informed choices and seek help;
- ensure that technology is selected, configured and used in ways that are proportionate to the setting's safeguarding and operational risks;
- establish clear routes for reporting, recording, escalating and learning from online safety concerns;
- support inclusive practice that reflects age, development, disability, communication needs, vulnerability and individual circumstances; and
- ensure that the setting's online safety arrangements remain current as technology, patterns of harm and statutory expectations change.

The setting recognises four broad areas of online risk: content, contact, conduct and commerce. These categories overlap and can be enabled or intensified by social media, gaming, messaging, live streaming, recommender systems, personal devices, artificial intelligence (AI), connected toys and devices, virtual or augmented environments and other emerging technologies.

Area	Examples
Content	Illegal, inappropriate or harmful content; pornography; sexual or violent material; hate content; misinformation and disinformation; self-harm or suicide content; extremist material; AI-generated or manipulated content.
Contact	Harmful interaction with other users; grooming; coercion; exploitation; harassment; sexual extortion; unsafe chatbots or AI companions; contact with adults or peers who pose a risk.
Conduct	Online behaviour that causes or increases harm, including bullying, harassment, abusive behaviour, sharing nudes or semi-nudes, non-consensual sharing, impersonation, image manipulation, doxxing, hacking or misuse of accounts, sharing passwords and accepting friend requests from unknown people.
Commerce	Gambling, scams, phishing, financial exploitation, inappropriate advertising, subscription or in-app purchase risks, fraud, identity theft and other commercial or financial harms.

2. Scope and application

This policy applies to all members of the setting community, including children and learners, employees, agency and temporary staff, governors, trustees, proprietors, volunteers, contractors, consultants, visitors and external providers where they have access to the setting's premises, technology, systems, accounts, information or children.

It applies to:

- setting-owned, managed or supplied devices, accounts, networks and services;
- personal devices where they are authorised to access setting information, systems or networks, or where their use affects safeguarding, behaviour or professional conduct;
- cloud services, educational platforms, apps, social media, messaging, AI tools and other online services used for setting business or learning;
- technology used on site, remotely, during educational visits, in residential provision where applicable, and on setting-managed devices used away from the site; and
- online conduct outside the setting where there is a safeguarding concern, a connection to the setting community, or a lawful basis for the setting to respond.

3. Online safety principles and whole-setting approach

The setting will apply the following principles:

- Safeguarding first: the welfare and best interests of children and learners are central to decisions about technology and online safety.
- Whole-setting responsibility: online safety is not owned by one individual or by the IT function; it requires leadership, safeguarding expertise, technical controls, curriculum, staff practice and family engagement.
- Prevention and education: technical controls will be combined with supervision, teaching, professional curiosity and opportunities for children to build resilience and digital literacy.
- Proportionate access: filtering, monitoring and other controls will seek to protect users without unnecessarily restricting legitimate teaching, learning, accessibility or support.
- Child-centred response: concerns will be considered in context, including the child's voice, age, development, vulnerability, relationships, motivation

and possible coercion.

- Inclusive practice: arrangements will take account of SEND, communication needs, assistive technology, EAL, care experience, trauma, mental health, exploitation risk and other relevant circumstances.
- Professional accountability: staff will use approved systems and maintain professional boundaries, including when working remotely or using social media and personal devices.
- Continuous improvement: incidents, near misses, audit findings, pupil voice, technological change and updated guidance will be used to strengthen policy, curriculum and controls.

4. Roles, leadership and accountability

The governing body, trust board, corporation or proprietor holds strategic responsibility for safeguarding and for ensuring that appropriate online safety arrangements are in place. Senior leaders are responsible for implementation and for ensuring that online safety is integrated into safeguarding, curriculum, behaviour, digital strategy, data protection, procurement and risk management.

The DSL leads safeguarding responsibility for online safety. The DSL should have sufficient understanding of the setting's filtering and monitoring arrangements, online risks and incident routes to identify and respond to concerns effectively. Technical staff or providers implement and maintain technical controls, provide evidence and explain limitations, but do not replace safeguarding judgement or leadership accountability.

At a high level:

- governors, trustees or proprietors seek assurance that the setting's online safety arrangements are effective and reviewed;
- the headteacher, principal or equivalent senior leader ensures this policy and linked procedures are implemented;
- a named senior leader is responsible for the strategic management of

filtering and monitoring, with support from the DSL and IT;
- the DSL leads the safeguarding response to online safety concerns and ensures relevant information is recorded and shared appropriately;
- the senior leader responsible for IT or digital strategy oversees digital governance and works with technical staff or providers on risk, procurement and assurance;
- the Data Protection Officer or data protection lead advises on privacy, lawful processing, DPIAs, records and personal data breaches;
- all staff follow the policy, supervise technology appropriately, maintain professional boundaries and report concerns promptly;
- children and learners are supported to use technology responsibly and to report worries or mistakes without fear of being ignored; and
- parents and carers are supported to understand the setting's expectations and how to seek help.

Detailed responsibilities, including assurance and reporting lines, are set out in the separate Roles and Responsibilities Schedule.

5. Education, curriculum and digital resilience

The setting will provide a planned, progressive and age-appropriate approach to online safety education. Teaching will be integrated across relevant curriculum areas and reinforced whenever technology is used, rather than relying solely on one-off events or assemblies.

The curriculum should enable children and learners, at an appropriate level, to understand:

- how to recognise safe, respectful and healthy online relationships and behaviour;
- how content is created, ranked, recommended, shared, altered and

monetised;

- how to assess the reliability of information, including misinformation, disinformation, manipulated media and AI-generated content;
- privacy, personal information, digital footprints, passwords, account security and the consequences of sharing information online;
- the risks of grooming, exploitation, coercion, bullying, harassment, hate, sexual harm, sexual extortion and financial scams;
- the implications of creating, requesting, storing, forwarding or sharing sexual images, including AI-generated or manipulated images;
- how algorithms, persuasive design, advertising, gambling-like features and in-app purchases can influence behaviour;
- how to use AI and emerging technologies critically, ethically, safely and in accordance with setting expectations;
- how to report harmful or illegal content and how to seek help from a trusted adult; and
- that online activity may have legal, disciplinary, reputational and wellbeing consequences.

Teaching will be adapted to the setting's phase and community. It will be sequenced so that children build on prior learning and are prepared for increasing independence. Sensitive topics will be taught in a way that prioritises safeguarding and allows children to ask questions and make disclosures safely.

The setting will use pupil or learner voice, safeguarding information, local patterns of concern and emerging risks to review the curriculum. External speakers or resources may be used where they add value, but they will complement rather than replace internal teaching.

6. Vulnerable children and learners

Some children and learners may face additional or different online risks, or may experience greater barriers to recognising, avoiding or reporting harm. Online

safety arrangements will therefore be adapted where necessary rather than assuming a single approach is suitable for all.

Children with SEND or communication needs may require accessible language, visual support, repetition, adapted interfaces, assistive technology or personalised teaching.

Children in care, previously looked-after children, children experiencing trauma or loss, and children with mental health needs may have additional vulnerabilities or patterns of online use that require sensitive support.

Children at risk of criminal or sexual exploitation may experience online grooming, coercion, financial exploitation, image-based abuse, sexual extortion or contact across multiple platforms.

Children with limited English proficiency may require adapted information and additional support to understand risks and reporting routes.

Reasonable adjustments and accessibility requirements will be considered when applying security, filtering, device or communication rules.

The DSL, SENCO or equivalent, pastoral staff, designated teacher, mental health leads, curriculum staff and technical staff should work together where individual needs affect online safety. Where appropriate, individual plans, risk assessments or reasonable adjustments will record how safe access will be supported.

7. Staff awareness, training and professional expectations

All staff must understand that technology is a significant component of many safeguarding and wellbeing issues and that online and offline harm may occur at the same time. Online safety will therefore be included in safeguarding induction and regular updates.

Training and awareness will ensure staff understand:

- the setting's online safety policy, reporting routes and linked procedures;
- the four areas of online risk and current patterns of harm relevant to the setting;
- the filtering and monitoring arrangements in place, including how concerns and alerts are escalated;
- safe and professional use of accounts, devices, communications, social media and AI;
- the need to protect personal, confidential and safeguarding information;
- the importance of supervision, professional curiosity and reporting concerns even where no technical alert is generated;
- how to respond to disclosures or harmful content without conducting their own investigation; and
- the additional risks and barriers that may affect vulnerable children.

Staff must only use authorised systems and services for organisational business, maintain professional boundaries, protect their accounts and devices, and follow the Staff Acceptable Use Agreement, Staff Online Safety Quick Guide, Cyber Security and Account Management Standard, Communications, Social Media and Image Use Procedure, AI and Emerging Technology Procedure and other relevant documents.

8. Working with parents and carers

Parents and carers play an important role in helping children develop safe and responsible online habits. The setting will work in partnership with families and will communicate clearly about its approach to online safety.

The setting will make this policy and relevant agreements available in accessible formats.

Parents and carers will be informed about the setting's filtering and monitoring

arrangements and about significant changes that affect children.

The setting will provide or signpost practical guidance on online risks, reporting routes, mobile devices, social media, AI and emerging technology.

Where an online safety incident involves a child, parents or carers will normally be involved at an appropriate stage unless doing so could place the child at greater risk, prejudice an investigation or conflict with advice from statutory agencies.

Parents and carers will be encouraged to discuss online safety with their child, support age-appropriate boundaries and contact the setting when concerns arise.

9. Reporting and responding to online safety concerns

All online safety concerns will be taken seriously. Staff must report safeguarding concerns to the DSL or safeguarding team promptly and must follow the setting's safeguarding procedures. Where there is a significant or immediate risk of harm then appropriate action must be taken without delay.

- The setting's response will be guided by the following principles:
- protect the child or person at risk and reduce further exposure or harm;
- listen carefully, avoid blame and do not promise confidentiality;
- do not conduct an unnecessary investigation or ask a child to repeatedly recount events;
- do not view, copy, print, forward, save or ask a child to send sexual imagery unless specifically required by an authorised safeguarding or law-enforcement process;
- preserve relevant evidence where this can be done safely and lawfully;
- consider whether the concern also involves behaviour, staff conduct, cyber security, data protection, criminal activity or another policy route;
- record safeguarding decisions, actions, referrals and rationale appropriately;

- involve parents or carers where appropriate and safe to do so;
- seek advice or refer to children's social care, police, Prevent/Channel, the local authority, the Internet Watch Foundation, CEOP, the ICO or other bodies where required; and
- review incidents to identify learning for policy, curriculum, supervision, technical controls and staff training.

Detailed decision-making, including responses to child-on-child sexual harm, making or sharing nudes or semi-nudes, child sexual abuse material, sexual or criminal exploitation, cyberbullying, radicalisation, harmful content, AI-generated imagery and other online incidents, is set out in the separate Incident Response Procedure and Local Safeguarding Contacts and Referral Schedule.

10. Filtering, monitoring and access to technology

The setting will provide a safe online environment through appropriate filtering and monitoring systems that are proportionate to the age and needs of users, the technologies in use and the setting's risk profile. Filtering and monitoring support safeguarding but do not replace professional judgement, supervision, education or the duty to report concerns.

The governing body or proprietor will ensure appropriate filtering and monitoring arrangements are in place and will seek assurance about their effectiveness.

A named senior leader will hold responsibility for the strategic management of filtering and monitoring, working with the DSL and technical staff or providers.

The effectiveness of filtering and monitoring will be formally reviewed at least once every academic year and after significant incidents, technology changes or identified weaknesses.

Checks will be recorded and will consider different user groups, devices, locations,

off-site use of managed devices and relevant AI or app-based activity.

Users will be informed, in age-appropriate and transparent ways, that setting systems and managed devices may be filtered, monitored and logged.

High-risk safeguarding alerts and routine monitoring reports will be managed through documented routes that reflect the setting's operating hours and safeguarding arrangements.

The setting will avoid blanket or excessive restrictions that unnecessarily limit legitimate teaching, learning, inclusion or access to support.

Detailed technical, operational and assurance requirements are set out in the Filtering and Monitoring Standard and Annual Assurance Checklist.

11. Cyber security and account security

Cyber security is essential to safeguarding, continuity of education, protection of personal data and the reliable operation of the setting. The setting will manage cyber security as an organisational risk rather than solely as a technical matter.

Accounts, access permissions and authentication will be appropriate to users' roles and risks.

Staff and other users must protect passwords, authentication methods, devices and organisational information.

Setting-owned or managed devices and systems will be securely configured, supported and updated.

Cloud services and third-party systems will be subject to appropriate due diligence and approval before organisational data is processed.

Backups, recovery arrangements and business continuity will reflect the importance of safeguarding, teaching, communication and administrative systems.

Suspected phishing, malware, account compromise, data breaches, lost devices and other cyber incidents must be reported promptly.

Where a cyber incident has safeguarding implications, the DSL will be involved and the concern may need to be managed through both cyber and safeguarding routes.

Detailed requirements for account security, Multi-Factor Authentication (MFA), devices, software, networks, backups, suppliers, incident response and assurance are set out in the Cyber Security and Account Management Standard.

12. Artificial intelligence and emerging technology

The setting recognises that AI and other emerging technologies can support education and administration but may also create safeguarding, data protection, intellectual property, equality, security and educational risks. AI will be managed as part of the setting's existing safeguarding and digital governance framework rather than as an isolated issue.

Only tools and uses that are appropriate to the user's age, role and purpose should be used for setting activity.

Staff and learners must follow setting expectations about approved tools, supervision and acceptable use.

Personal, confidential, special category or safeguarding information must not be entered into AI systems unless the use has been explicitly approved and the relevant data protection requirements have been met.

AI-generated output must be checked critically for accuracy, bias, fabricated information, harmful content and appropriateness before it is relied upon or shared.

The setting will consider intellectual property, copyright, transparency and

assessment integrity when using AI-generated material.

Safeguarding risks may include unsafe chatbots or companions, manipulation, impersonation, deepfakes, nudification, AI-generated sexual imagery, grooming, harmful prompts and rapid generation or amplification of harmful content.

AI-related concerns will be reported and responded to through the same safeguarding principles as comparable non-AI concerns.

New tools or significant changes to existing services will be risk-assessed before adoption, with input from safeguarding, digital/IT and data protection roles as appropriate.

Detailed rules for approved use, age restrictions, staff and learner use, procurement, privacy, assessment, copyright and incident handling are set out in the AI and Emerging Technology Procedure.

13. Communications, social media and image use

Digital communication must be professional, transparent and consistent with safeguarding and staff conduct expectations. The setting will define approved communication channels and will not rely on personal accounts or informal arrangements where organisational systems should be used.

Staff will communicate with children, learners and parents only through approved organisational channels.

Official social media accounts will be authorised, managed and monitored in accordance with setting procedures.

Images, video, audio and livestreams will be captured, stored, shared and published lawfully and with appropriate regard to safeguarding, privacy and consent or other lawful basis.

Staff must report unsolicited or concerning contact, impersonation, fake accounts, manipulated images, deepfakes or other misuse of identity.

Remote and live online interactions will use approved platforms and maintain the same professional boundaries and safeguarding expectations as face-to-face activity.

Detailed expectations are set out in the Communications, Social Media and Image Use Procedure and relevant Staff Acceptable Use Agreement.

14. Mobile phones, personal devices and wearable technology

The setting will maintain clear rules for mobile phones, personal devices and wearable or smart technology. The rules will reflect the setting type, age of learners, behaviour expectations, accessibility needs and statutory requirements applicable to the provision.

Schools to which the statutory mobile phone guidance applies will maintain a policy that prohibits pupil use of mobile phones throughout the school day, subject to permitted exceptions and reasonable adjustments.

Post-16, college, early years and other settings will adopt proportionate arrangements that reflect their legal framework and operational context.

Staff personal-device use must remain consistent with professional conduct, confidentiality, safeguarding and image-use expectations.

Visitors and volunteers will be informed of relevant restrictions before or on arrival.

Personal mobile data or other workarounds must not be used to circumvent the setting's filtering, monitoring or security controls.

Wearable devices, smart watches and other connected technologies will be included where they create equivalent communication, recording, safeguarding or security risks.

Any search, confiscation or examination of a device will be undertaken only in accordance with the lawful powers and guidance applicable to the setting.

Detailed setting rules, including exceptions, reasonable adjustments and consequences, are set out in the Mobile Phone and Personal Device Policy.

15. Data protection, privacy and information sharing

Online safety activity often involves personal data, including monitoring logs, account information, photographs, safeguarding records, incident information and technical evidence. The setting will process this information lawfully, fairly, securely and proportionately.

Personal information will be collected, used, shared, retained and disposed of in accordance with the setting's data protection framework and retention arrangements.

Access to safeguarding, monitoring and security information will be restricted to those who need it for safeguarding, security, legal, operational or assurance purposes.

Data Protection Impact Assessments (DPIA) will be completed or updated where required, including for filtering and monitoring solutions and other technology that creates a high risk to individuals' rights and freedoms.

Safeguarding information may be shared without consent where there is a lawful basis and sharing is necessary and proportionate to protect a child or another person.

Staff must not allow uncertainty about data protection to prevent appropriate safeguarding information sharing; advice should be sought from the DSL and DPO or data protection lead where necessary.

Third-party providers will be subject to appropriate data protection and security due diligence, contractual arrangements and oversight.

16. Community use, third-party providers and external access

Where the setting hires or lets premises, commissions activities, provides network access to external users, or works with third-party education, tuition, community or extracurricular providers, safeguarding arrangements must remain clear.

Contracts, transfer-of-control arrangements or service agreements will identify relevant safeguarding, online safety, data protection and technology responsibilities.

Where a provider operates independently, the setting will seek appropriate assurance about safeguarding policies, staff conduct, communications, online safety and, where relevant, filtering and monitoring.

External users who access setting networks or devices must follow local access and acceptable-use requirements.

Third-party services and suppliers that process organisational information or have privileged technical access will be subject to due diligence and proportionate assurance.

17. Monitoring, assurance and review

The setting will review this policy at least annually and sooner when required. Review is a governance and safeguarding process, not simply an editorial exercise.

A review may be triggered by:

- changes to statutory or departmental guidance;
- a significant safeguarding, cyber, data protection or technology incident;
- changes to filtering, monitoring, network infrastructure, device strategy or outsourced services;
- introduction of new or emerging technologies, including AI;
- patterns identified through safeguarding records, monitoring data, behaviour incidents or pupil voice;
- changes to the age profile, provision, accessibility needs or risk profile of the setting; or
- findings from audit, inspection, assurance activity or complaints.

Leaders will seek proportionate evidence that key controls and procedures are operating as intended. Governors, trustees, corporations or proprietors will receive appropriate assurance on online safety risks, incidents, training, filtering and monitoring, cyber security, curriculum and improvement actions.

The setting will involve staff, children and learners, and parents or carers in review where this is useful and proportionate. Accessibility and equality implications will be considered when policies, systems or controls are changed.

18. Related policies, procedures and supporting documents

This core policy should be read alongside the setting's wider safeguarding and digital governance framework, including:

- Child Protection and Safeguarding Policy;
- Staff Behaviour / Code of Conduct and low-level concerns arrangements;
- Behaviour and Anti-Bullying Policies;
- Acceptable Use Agreements for pupils, parents/carers, staff and visitors;

- Staff Online Safety Quick Guide;
- Roles and Responsibilities Schedule;
- Incident Response Procedure;
- Filtering and Monitoring Standard and Annual Assurance Checklist;
- Cyber Security and Account Management Standard;
- AI and Emerging Technology Procedure;
- Communications, Social Media and Image Use Procedure;
- Mobile Phone and Personal Device Policy;
- Data Protection Policy, privacy notices and retention schedule;
- Business Continuity and Cyber Incident Response arrangements;
- Local Safeguarding Contacts and Referral Schedule; and
- relevant curriculum policies, including Relationships Education / RSE, Health Education, Computing and PSHE where applicable.