A black and white logo

AI-generated content may be incorrect.**Windy Nook Primary School**

**Online Safety Policy**

Windy Nook Primary School is committed to safeguarding all members of our school community in the digital environment. This Online Safety Policy outlines our approach to ensuring the safe, responsible, and respectful use of digital technologies, in line with statutory guidance and recognised best practices.

This policy applies to all individuals who access or use the school’s digital systems, both on and off-site. This includes staff, pupils, volunteers, parents and carers, visitors, and community users. It also covers the use of personal digital devices when used in connection with school activities.

Any incidents involving inappropriate online behaviour will be addressed in accordance with this policy, alongside the school’s Behaviour and Anti-Bullying Policies. Where incidents occur outside of school and are brought to our attention, we will inform parents and carers as appropriate.

**Key Aims of the Online Safety Policy**

* **Promote Safe Use**: Establish clear expectations for the safe and responsible use of digital technologies for learning, communication, and administration.
* **Define Responsibilities**: Outline the roles and responsibilities of staff and other stakeholders in implementing and upholding the policy.
* **Staff Guidance**: Provide guidance for staff on protecting themselves and the school when using digital tools, and how to support pupils in navigating the digital world safely.
* **Pupil Preparation**: Equip learners with the knowledge and skills to become safe, respectful, and responsible users of online technologies.
* **Incident Management**: Set out clear procedures for identifying, reporting, responding to, and recording online safety concerns, including access to external support where needed.
* **Acceptable Use Agreements**: Support the policy with a series of tailored Acceptable Use Agreements for different user groups.
* **Accessibility**: Ensure the policy is introduced to all staff during induction and remains accessible via the school’s SharePoint platform.
* **Ongoing Review**: Ensure the policy is regularly reviewed and updated collaboratively, reflecting emerging technologies, trends, and incidents.

## Key Responsibilities

* The Headteacher and Senior Leaders are responsible for fostering a culture of safeguarding and ensuring staff are trained in online safety.
* Governors approve and review the Online Safety Policy and appoint an Online Safety Governor.
* The Online Safety Lead manages day-to-day online safety issues and coordinates training and reporting.
* The Designated Safeguarding Lead (DSL) leads on safeguarding, including online safety.
* Teaching Staff embed online safety in the curriculum and model responsible behaviour.
* Technical Staff ensure secure infrastructure and filtering/monitoring systems.
* Learners follow acceptable use agreements and report concerns.
* Parents and Carers support safe use of technology at home and engage with school initiatives.

## Governors

Governors play a key role in ensuring the school meets its safeguarding duties, including online safety, as outlined in the DfE’s *Keeping Children Safe in Education* guidance. Governors support efforts to involve parents, carers, and the wider community in promoting safe online behaviours.

## Responsibilities:

* Policy Oversight: Approve and regularly review the Online Safety Policy.
* Designated Role: One governor is appointed as the Online Safety Governor, responsible for:
* Meeting regularly with the Online Safety Lead.
* Monitoring the implementation of online safety education and staff training.
* Reporting updates and concerns to the full governing body.

## Online Safety Lead

The Online Safety Lead is responsible for the day-to-day management of online safety across the school. This includes:

* Working closely with the Designated Safeguarding Lead (DSL) to address online safeguarding concerns.
* Leading the development and review of online safety policies and ensuring staff are trained and aware of reporting procedures.
* Coordinating the online safety curriculum with curriculum leaders.
* Logging and analysing incidents (via Impero) to inform future improvements.
* Providing training and guidance to staff, governors, parents, and learners.
* Liaising with technical staff (Gateshead SIS), the local authority, and the Online Safety Governor.
* Reporting regularly to the senior leadership team and attending relevant meetings.

Guidance: https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

## Designated Safeguarding Leads (DSL)

The DSL holds overall responsibility for safeguarding and child protection, including online safety. This role must be clearly defined in their job description, as required by DfE guidance.

Key Responsibilities:  
Lead on all safeguarding matters, including online risks.  
Be trained to understand and respond to online safety threats such as:  
 • Sharing of personal data  
 • Access to illegal or harmful content  
 • Inappropriate online contact  
 • Grooming and exploitation

Guidance: https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

## Subject Leaders

Curriculum Leads, particularly the Computing Subject Lead and Online Safety Lead, are responsible for delivering a structured and age-appropriate online safety education programme. This includes:

* Planning and delivering dedicated online safety lessons.
* Integrating online safety into PSHE, SRE, assemblies, and pastoral sessions.
* Promoting national initiatives such as Safer Internet Day and Anti-Bullying Week. All teaching and support staff are expected to actively promote and model safe, responsible, and professional online behaviour.

Their key responsibilities include:

* Stay Informed: Keep up to date with online safety trends, school policies, and safeguarding procedures.
* Embed Online Safety: Integrate online safety into the curriculum and model responsible digital behaviour in all interactions.
* Use Approved Platforms: Communicate with learners and parents/carers only through school-approved platforms.
* Maintain Professionalism: Ensure all digital communication is appropriate in tone and content. Personal email, messaging apps, or social media must not be used for school-related communication.
* Protect Professional Reputation: Use personal social media responsibly, maintaining a professional image that reflects the values of the school.
* Supervise and Safeguard: Monitor learners’ use of digital devices and report any concerns to the Designated Safeguarding Lead (DSL).
* Follow Safeguarding Protocols: Adhere to safeguarding guidelines during live-streamed or video-conferenced lessons.
* Challenge Inappropriate Behaviour: Take a zero-tolerance approach to online bullying, harassment, and discrimination.
* Report Concerns: Immediately report any communication that is offensive, discriminatory, threatening, or makes anyone feel uncomfortable. Do not respond to such messages.
* Follow Publishing Guidelines: Ensure all online content (e.g. school website, social media) complies with school policies and has the necessary permissions.

## Online Safety Education

The school delivers a comprehensive online safety curriculum using, integrated across subjects and supported by national initiatives such as Safer Internet Day. Staff receive regular training, and learners are taught to be responsible digital citizens.

# Reporting and Responding to Online Safety Incidents

The school is committed to maintaining a safe online environment and recognises that incidents may occur both on and off-site that impact the school community. To ensure effective response and accountability, the school will:

## Clear Reporting Procedures

* Maintain clear, accessible reporting routes aligned with safeguarding, whistleblowing, complaints, and managing allegations policies (via CPOMS).
* Ensure all staff, students, and stakeholders understand how to report online safety concerns using CPOMS.
* Respond to reports promptly and in line with safeguarding protocols.

## Staff Training and Escalation

* Ensure the Designated Safeguarding Lead (DSL), Online Safety Lead, and relevant staff are trained to manage online safety risks.
* Escalate incidents involving suspected illegal activity or serious harm through safeguarding procedures immediately.
* Report concerns about staff misuse to the Headteacher, or to the Chair of Governors and local authority if the Headteacher is involved (see Whistleblowing Policy).

## Device and Content Review Protocol

Where no illegal activity is suspected, device checks may be conducted under the following conditions:

* At least one senior staff member must be present to ensure transparency and protection.
* Use a designated device not accessible to students, which can be handed to police if needed.
* Ensure secure internet access for investigation, with all activity monitored and logged.
* Record URLs and describe concerning content; screenshots may be taken, signed, and attached to the report.
* Following investigation, determine if the concern is substantiated and take appropriate action, which may include:

- Internal disciplinary measures

- Local authority involvement

- Police action

## Support and Communication

* Foster a culture where individuals feel confident that reports will be taken seriously and handled effectively.
* Provide support for those affected, including peer support and access to external resources (e.g. CEOP, Professionals Online Safety Helpline, Reporting Harmful Content).
* Log all incidents on CPOMS and provide feedback to those involved on outcomes and next steps.

# Learning and Prevention

Share lessons learned from incidents with:

- Staff – through briefings and training

- Students – via assemblies and curriculum

- Parents/Carers – through newsletters, social media, and the school website

- Governors – in safeguarding updates

- External agencies – as appropriate

## Network Manager / Technical Staff

Gateshead SIS ensures the school’s digital systems are secure and well-managed. Their responsibilities include:

* Following Online Safety and Technical Security Policies.
* Protecting the network from misuse or cyber threats.
* Meeting local authority safety standards.
* Managing secure access to devices and systems.
* Staying informed on online safety trends and sharing updates.
* Monitoring usage and reporting concerns to the DSL.
* Maintaining filtering and monitoring tools (e.g. Impero) with shared accountability.

## Learners

Learners must use school technology responsibly, following the Acceptable Use Agreement. They should:

* Report any misuse or harmful content.
* Know how to get help if they feel unsafe online.
* Understand that online safety applies both in and out of school, especially when linked to school activities.

## Parents and Carers

Parents and carers support their child’s safe technology use. The school helps by:

* Sharing the Online Safety Policy and Acceptable Use Agreements.
* Providing guidance on social media and digital permissions.
* Offering updates through newsletters, events, and campaigns.

Parents are encouraged to:

- Promote safe and respectful online behaviour at home.

- Set clear rules and boundaries for technology use.

- Monitor their child’s online activity and discuss any concerns.

- Encourage open conversations about digital wellbeing and online experiences.

- Support the school’s policies by ensuring personal devices are used appropriately and only when permitted.

## School Actions

Most online safety incidents in school are likely to involve inappropriate rather than illegal behaviour. It is essential that these are addressed swiftly, proportionately, and transparently. The school is committed to ensuring that all incidents are managed in line with the School Behaviour Policy, and that the wider school community is reassured that appropriate action has been taken.  
  
Relevant guidance: https://www.gov.uk/government/publications/teaching-online-safety-in-schools

## Online Safety Education Programme

Online safety is embedded across the curriculum and reinforced by staff in all subject areas. The programme is designed to be broad, progressive, and inclusive, and is delivered through:

* A planned curriculum for all year groups using resources tailored to our school context.
* Age-appropriate lessons that build on prior knowledge.
* Contextualised learning with clear objectives and measurable outcomes.
* Effective planning and assessment to meet learner needs and track progress.
* Integration of digital competency across subjects such as PSHE, SRE, and Literacy.
* Participation in national initiatives like Safer Internet Day and Anti-Bullying Week.
* Adaptations to ensure accessibility for learners with additional needs or English as an additional language.
* Pre-planned internet use with guided access to approved sites and clear procedures for managing unsuitable content.
* Regular review and updates to maintain high-quality learning and outcomes.

## Contribution of Learners

The school values the digital knowledge and experiences of its learners. Their input helps shape our online safety strategy and supports their personal development. We actively encourage learner voice and participation in shaping a safer digital environment.  
  
Relevant guidance: https://www.gov.uk/government/collections/statutory-guidance-schools

## Staff

All staff are trained to understand their responsibilities in promoting and maintaining online safety. Training includes:

* A structured programme of online safety and data protection training via Clennell Education Solutions, regularly updated.
* Inclusion in the school’s annual safeguarding and data protection training.
* Induction training for new staff covering policy, acceptable use, classroom management, professional conduct, and online reputation.
* Ongoing updates and discussions in staff meetings.
* Access to support and guidance from the Online Safety Lead or designated staff.

# Filtering and Monitoring

The school ensures online safety through a robust filtering and monitoring strategy:

* Policy & Oversight: Filtering policies are set and reviewed by senior leaders and technical staff.
* Partnership: Content access is managed with Gateshead SIS.
* Illegal Content: Blocked using the IWF CAIC list and Home Office guidance.
* Reporting: Clear procedures exist for reporting issues and requesting filter changes.
* Monitoring Tools: All network activity is monitored via Impero.
* User Awareness: Users are informed that monitoring is in place.
* Designated Online Safety Lead: A staff member oversees monitoring and safeguarding alerts.
* Review & Action: Logs and alerts are regularly reviewed and acted upon.

## Monitoring Includes:

* Classroom supervision
* Internet use logging
* Third-party support via Impero

The school follows UK Safer Internet Centre guidance and uses a risk-based approach to ensure effective protection.

# Technical Security

The school’s technical infrastructure is managed to meet current security standards and best practices. Regular audits and reviews ensure systems remain secure and compliant.

## System Security

* Infrastructure Protection: Servers, wireless access points, and cabling are securely housed with restricted physical access.
* User Credentials: All users are responsible for safeguarding their login credentials. Sharing passwords is strictly prohibited. Any suspected security breach must be reported immediately.
* Password Management:  
   -All systems are protected by strong, unique passwords.  
   - Passwords are issued and managed by Gateshead SIS, with complexity requirements including length, capital letters, and special characters.  
   - Users must update their passwords regularly.  
   - For Key Stage 1 learners, usernames and passwords may be stored securely in electronic or paper form.  
   - Password complexity increases progressively for learners from Key Stage 2 onwards.

## Software and Network Security

* Gateshead SIS ensures all software is properly licensed and regularly updated with security patches.
* Firewalls, routers, wireless systems, and endpoints are protected against threats through robust security measures and up-to-date antivirus software.
* Temporary access for guests (e.g., supply teachers, visitors) is managed via restricted, generic accounts.  
  - Policies govern:  
   - Personal use of school devices (see Acceptable Use Policy)  
   - Installation of software and executable files  
   - Use of removable media (e.g., USB drives)  
   - Secure handling and encryption of personal data

# Mobile Technologies

* The Acceptable Use Agreements outline expectations for mobile device usage.
* Only school-owned devices are permitted to access the school’s network and systems.

# Social Media

## Safeguarding Measures

Personal information must not be published online.  
Staff and learners receive training on:  
 - Acceptable use  
 - Age restrictions  
 - Online safety and privacy settings  
 - Data protection  
 - Reporting concerns

## Staff Responsibilities

* Do not reference learners, parents, or colleagues on personal social media.
* Avoid discussing personal matters related to the school community online.
* Personal views must not be presented as those of the school.
* Maintain secure privacy settings on personal accounts.
* Model positive and responsible social media behaviour.

## Official School Accounts

* Clear administration and moderation processes involving at least two staff members
* A code of conduct for users
* Reporting and response procedures for misuse
* Alignment with school disciplinary policies

## Personal Use Guidelines

* Personal social media use that references or impacts the school must include a disclaimer clarifying the individual is not speaking on behalf of the school.
* Personal use that does not affect the school is outside the scope of this policy.
* Excessive or inappropriate use during school hours may result in disciplinary action.
* Reasonable access to personal social media is permitted during school hours.

# Data Protection

## Governance and Compliance

* Maintains a comprehensive Data Protection Policy.
* Demonstrates compliance with the data protection principles.
* Is registered with the Information Commissioner’s Office (ICO)
* Has appointed a qualified Data Protection Officer (DPO).

## Data Management

* Maintains a Record of Processing Activities (ROPA).
* Maintains an Information Asset Register.
* Collects and retains only the minimum necessary personal data.
* Ensures data is accurate and up to date.
* Provides clear Privacy Notices to all stakeholders.

## Individual Rights and Risk Management

* Supports all data subject rights.
* Conducts Data Protection Impact Assessments (DPIAs).
* Ensures compliant contracts with third-party data processors.
* Shares data lawfully and securely.
* Has procedures for secure deletion and disposal of data.

## Data Breach Management

* Has an incident response policy.
* Reports notifiable breaches to the ICO within 72 hours.

## Freedom of Information

* Maintains a Freedom of Information (FOI) Policy.

## Training and Awareness

* Provides mandatory data protection training for all staff.
* Offers role-specific training where required.

## Data Security on Devices and Media

* Data must be encrypted and password protected.
* Devices must be secured and protected by antivirus software.
* Data must be securely deleted when no longer needed.

## Staff Responsibilities

* Handle personal data with care.
* Recognise and report data breaches.
* Support data subjects in understanding their rights.
* Use only encrypted storage.
* Never transfer school data to personal devices.
* Use secure, password-protected devices.
* Transfer data using secure methods.

## Filtering and Monitoring

The school uses Impero and works with Gateshead SIS to ensure robust filtering and monitoring of internet use. Monitoring logs are reviewed regularly and safeguarding alerts are prioritised.

# Evaluating Impact and Outcomes

## Monitoring and Evaluation

* Regular reviews of online safety incident logs, behaviour reports, and stakeholder surveys.
* Findings reported to school leadership and Governors.
* Policies updated based on evidence and professional dialogue.

## Relevant Government Guidance

The policy aligns with the following UK government guidance:

* Teaching online safety in schools: https://www.gov.uk/government/publications/teaching-online-safety-in-schools
* Final Statement of Strategic Priorities for Online Safety: https://www.gov.uk/government/publications/statement-of-strategic-priorities-for-online-safety/final-statement-of-strategic-priorities-for-online-safety
* Keeping children safe in education: <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

## Children’s Rights and Online Safety

This policy supports the following UNCRC articles:  
- Article 12: Right to be heard.  
- Article 13: Right to seek and share information.  
- Article 16: Right to privacy.  
- Article 17: Right to access safe information.  
- Article 19: Right to protection from harm.  
- Article 28: Right to education.  
- Article 34: Right to protection from sexual abuse.  
- Article 39: Right to support after harm.

**Appendix 1**

**Glossary of Online Safety Terms**

**Acceptable Use Agreement (AUA)**  
A set of rules outlining how users (staff, pupils, parents) are expected to behave when using school technology and digital platforms.

**CPOMS**  
A secure online system used by schools to record and manage safeguarding, wellbeing, and behaviour incidents.

**DSL (Designated Safeguarding Lead)**  
A senior member of staff responsible for overseeing safeguarding and child protection, including online safety.

**DPO (Data Protection Officer)**  
An appointed individual responsible for ensuring the school complies with data protection laws and manages personal data securely.

**DPIA (Data Protection Impact Assessment)**  
A process to identify and minimise data protection risks when handling personal data, especially for new projects or technologies.

**Filtering and Monitoring**  
Systems used to restrict access to harmful or inappropriate online content and to track user activity for safeguarding purposes.

**Gateshead SIS**  
The local authority’s Schools IT Service, which provides technical support, infrastructure management, and online safety tools.

**Impero**  
A monitoring and classroom management tool used to track digital activity, flag safeguarding concerns, and support safe device use.

**Online Safety Lead**  
A designated staff member responsible for coordinating the school’s online safety strategy, training, and incident response.

**ROPA (Record of Processing Activities)**  
A document that outlines how personal data is processed, stored, and shared within the school.

**Safeguarding**  
The process of protecting children from abuse, harm, and neglect, including risks posed by digital technologies.

**Social Media Code of Conduct**  
Guidelines for staff and pupils on responsible use of social media, including privacy, professionalism, and safeguarding.

**UNCRC (United Nations Convention on the Rights of the Child)**  
An international agreement that outlines children’s rights, including the right to safety, privacy, and education in digital spaces.