DONAGHADEE PRIMARY SCHOOL
& NURSERY UNIT

ONLINE SAFETY POLICY

Learning, caring and growing together

1. Purpose and Scope

This policy sets out how Donaghadee Primary School & Nursery Unit provides a safe, responsible and inclusive digital environment. Online safety is treated as an integral part of safeguarding, child protection, curriculum provision, behaviour, staff conduct, data protection and cyber security, rather than as a stand-alone technical matter.

The policy applies to all use of digital technology connected with the school, whether on school premises or elsewhere, including C2k services, school-managed devices, personal devices authorised for school use, online learning platforms, email, messaging, social media, cloud services, video calls, artificial intelligence tools and published digital content.

2. Aims

- protect pupils and adults from online harm while enabling positive, creative and educational use of technology;
- ensure that safeguarding responsibilities remain the same online and offline;
- develop pupils' digital literacy, critical thinking, privacy awareness, respectful communication and help-seeking skills;
- establish clear expectations for acceptable use, filtering, monitoring, reporting and response;
- ensure personal data and school systems are handled securely and lawfully;
- work in partnership with parents, carers, C2k, the Education Authority and relevant safeguarding agencies; and
- review provision in response to emerging technology, patterns of harm and updated guidance.

3. Guiding Principles

- The best interests, dignity and welfare of the child are central to decision-making.
- Pupils will be supported and listened to. They will not be blamed for reporting an online concern.
- Online incidents will be considered through a safeguarding lens as well as through behaviour and technical procedures.
- Filtering and monitoring support safeguarding but do not replace education, supervision, professional curiosity or effective reporting.
- Responses will be proportionate, inclusive and sensitive to age, development, additional needs and vulnerability.
- The school will promote respectful, lawful and ethical use of digital technology.

4. Roles and Responsibilities

Board of Governors

- Approves this policy and receives assurance that online safety arrangements are implemented and reviewed.
- Ensures that safeguarding, data protection and cyber-security responsibilities are appropriately overseen.
- Challenges and supports leaders regarding staff training, filtering and monitoring, incident learning and risk management.

Principal

- Has overall responsibility for implementation and for ensuring that online safety is integrated with safeguarding and school improvement.

- Ensures that concerns are managed under the appropriate safeguarding, disciplinary, complaints, data protection or technical procedure.
- Ensures access to suitable training, advice and resources.

Designated Teacher / Deputy Designated Teachers

- Lead the safeguarding response where technology is involved.
- Ensure concerns are recorded, assessed, referred and followed up in line with the school Safeguarding and Child Protection Policy.
- Consider whether a concern indicates wider risk to other pupils or adults.

Online Safety / ICT Co-ordinator

- Coordinates curriculum provision, staff updates and policy implementation.
- Works with school leaders and C2k to review filtering, monitoring and technical controls.
- Maintains awareness of current EA, DE, C2k, Safer Schools NI, CEOP and UK Safer Internet Centre resources.

All staff, volunteers and contractors

- Follow the Staff Code of Conduct, Acceptable Use expectations and safeguarding procedures.
- Maintain professional boundaries and use approved systems for school business.
- Report concerns, suspected breaches, harmful content, device loss or unusual system activity promptly.
- Use professional judgement when selecting digital resources and supervise pupils appropriately.

Pupils

- Follow age-appropriate Online Safety Rules and Acceptable Use expectations.
- Treat others respectfully, protect passwords and personal information, and report anything worrying or unsafe.
- Use school technology for agreed educational purposes and cooperate with reasonable checks or investigations.

Parents and carers

- Support the school's online safety expectations and discuss safe, respectful technology use at home.
- Inform the school promptly about online issues that may affect a pupil's safety, wellbeing, attendance or learning.
- Make informed choices about consent for images and digital platforms.

5. Education and Curriculum

Online safety will be taught progressively and revisited throughout the year through the curriculum, PDMU, assemblies, pastoral work, anti-bullying learning and relevant events. Teaching will be age-appropriate, inclusive and responsive to current issues.

- privacy, personal information, passwords and digital footprints;
- respectful communication, consent, healthy boundaries and online reputation;
- recognising unreliable information, manipulated media, scams and persuasive design;
- responding to bullying, harmful contact, inappropriate content and pressure from others;
- copyright, ownership, appropriate attribution and responsible creation of content;
- balanced technology use, digital wellbeing and knowing when to seek help;
- safe and ethical use of generative artificial intelligence, including checking accuracy, protecting personal data, acknowledging assistance and following teacher instructions.

Pupils will be taught practical reporting routes, including speaking to a trusted adult, using platform reporting tools where appropriate, and accessing recognised support services. Teaching will emphasise that telling an adult is the right action.

6. Filtering, Monitoring and Supervision

Internet access is provided through the C2k managed service. The school recognises that no technical control is completely effective and therefore combines filtering and monitoring with education, supervision, clear routines and prompt reporting.

- Access to the internet will have a clear educational purpose and be appropriately supervised.
- Staff will report blocked legitimate content, suspected over-blocking, under-blocking or concerning search activity through agreed school/C2k routes.
- Leaders will periodically review whether filtering and monitoring arrangements remain suitable for the age and needs of pupils, the devices used and the school's risk profile.
- Pupils and staff will be informed that use of school networks, accounts and devices may be monitored in accordance with law, policy and C2k arrangements.
- Attempts to bypass security controls, use unauthorised proxy services or access another user's account are prohibited.

7. Acceptable Use of Systems and Devices

- Users must use their own authorised account and keep credentials confidential.
- Strong passwords must be used and changed when compromise is suspected. Multi-factor authentication must be used where provided.
- Software, browser extensions, apps and cloud services may be installed or used only where authorised.
- Personal data must not be stored on unapproved removable media, personal accounts or personal devices.
- School equipment remains school property and must be used carefully, securely and for authorised purposes.
- Portable devices must be locked when unattended and stored securely. Loss, theft or damage must be reported immediately.
- Pupils may not use personal phones or smart devices during the school day unless specifically authorised for an individual need or agreed activity.
- Staff use of personal devices must comply with the Staff Code of Conduct and must not compromise supervision, confidentiality or professional boundaries.

8. Email, Messaging, Video Calls and Online Platforms

- Only approved school/C2k accounts and platforms will be used for school communication and learning.
- Communication with pupils and families must be professional, transparent and capable of appropriate oversight.
- Pupils must report messages or material that are worrying, offensive, threatening or unexpected.
- Video calls will use approved platforms, appropriate settings and suitable supervision. Staff will consider the visibility of names, backgrounds, shared screens and recordings.
- Recordings, screenshots or redistribution of online sessions are not permitted unless authorised and lawful.
- Confidential or personal information must be shared only with authorised recipients and by an appropriate secure method.

9. Social Media and Public Communications

- Official school social media accounts will be authorised, administered and reviewed by designated staff.
- Staff must maintain professional boundaries and must not connect with current pupils through personal social media accounts.
- Personal use by staff must not bring the school into disrepute, disclose confidential information or undermine professional responsibilities.
- Only approved content may be published on behalf of the school. Comments and messages requiring a safeguarding response will be preserved and escalated.
- Parents and carers will be reminded not to post images or information about other children without permission and not to use online spaces to raise confidential school concerns.

10. Images, Video, Pupil Work and Consent

- Consent choices will be recorded through the school's current data-capture and privacy arrangements and may be withdrawn.
- Images and recordings will be taken using school-approved equipment and stored in approved locations.
- Publication will use the minimum information necessary. A pupil's full name will not normally be linked publicly with an identifiable image.
- Images will be respectful, appropriate and consistent with the purpose for which consent was obtained.
- Staff will consider location information, uniforms, name badges, background details and other identifiers before publication.
- External organisations may use pupil images or work only when appropriate permission and data protection arrangements are in place.

11. Artificial Intelligence and Emerging Technology

The school will take a cautious, educational and proportionate approach to generative AI and emerging technologies.

- No pupil or staff personal data, confidential school information, safeguarding information or unpublished assessment material may be entered into an unapproved AI service.
- AI output must be checked for accuracy, bias, suitability, copyright and safeguarding risk before use.
- Staff remain professionally accountable for materials, decisions and communications produced with AI assistance.
- Pupils may use AI only when directed and supervised, with expectations about acknowledgement, originality and appropriate support made clear.
- AI-generated or manipulated content used to deceive, bully, impersonate or cause harm will be managed under safeguarding and behaviour procedures.

12. Data Protection and Cyber Security

- Personal data will be processed in accordance with the school's Data Protection Policy, privacy notices and EA guidance.
- Users must verify recipients before sending information and use secure sharing methods for sensitive or personal data.
- Suspicious links, unexpected login prompts, phishing attempts, malware warnings and unusual account activity must be reported immediately and not forwarded unnecessarily.
- Critical data will be stored and backed up through approved systems. Security updates must not be disabled or delayed without authorisation.

- A suspected personal data breach will be contained and reported immediately to the Principal and the school's data protection contact so that required assessment and notification can take place.

13. Responding to Online Safety Concerns

Any member of the school community may report an online safety concern to a trusted member of staff. Staff must not investigate beyond what is necessary to establish immediate safety and preserve relevant information.

1. Protect: address immediate safety, provide reassurance and avoid blame.
2. Report: notify the Designated Teacher/Deputy Designated Teacher or Principal without delay where safeguarding may be involved.
3. Record: make a clear, factual and timely record using the school's safeguarding or incident system.
4. Preserve: retain relevant usernames, links, dates, messages or screenshots only where safe, lawful and necessary. Do not unnecessarily copy or circulate harmful material.
5. Assess and refer: follow the Safeguarding and Child Protection Policy, including consultation or referral to the appropriate statutory service where required.
6. Contain and recover: involve C2k/EA technical or data protection support for account, network, device or data incidents.
7. Support and review: provide appropriate support, communicate with parents/carers when safe and appropriate, and identify lessons for curriculum, supervision or controls.

Where an allegation concerns an adult working with children, the Principal will follow the school's safeguarding procedures for allegations against staff. Where the concern relates to the Principal, it will be reported to the Chair of Governors. Emergency services should be contacted where there is an immediate risk of serious harm.

14. Online Bullying and Harmful Behaviour

Online bullying, harassment, impersonation, threats, exclusion, harmful sharing or misuse of images will be addressed consistently with the Positive Behaviour, Anti-Bullying and Safeguarding and Child Protection Policies. The school may respond to behaviour occurring outside school where it affects the safety, wellbeing or education of pupils or the orderly running of the school.

Responses will consider the needs of the child who has experienced harm, the child responsible, bystanders and the wider peer group. Restorative or educational approaches may be used where appropriate, but not as a substitute for safeguarding action.

15. Vulnerability, Inclusion and Additional Needs

Some pupils may face additional online risks or may require adapted teaching and reporting routes. The school will consider communication needs, sensory needs, cognition and learning, social understanding, emotional wellbeing, family context and previous experiences. Visual supports, repetition, accessible language, trusted-adult plans and targeted teaching will be used where helpful.

16. Parents, Carers and Community Information

- The school will share relevant updates through newsletters, the school website, ClassDojo and Safer Schools NI.
- Parents and carers will be encouraged to have regular, calm conversations about online life, agree boundaries, use available parental controls and know how to report concerns.
- The school may signpost families to EA, Safer Schools NI, CEOP, Childline, PSNI, SBNI and UK Safer Internet Centre resources as appropriate.

- Concerns about school practice should be raised through the school's complaints procedure rather than through public online discussion.

17. Staff Training and Induction

- Online safety will form part of safeguarding induction for new staff, governors, volunteers and relevant contractors.
- All staff will receive regular updates on emerging risks, reporting expectations, approved platforms, data protection and cyber security.
- Training needs will be informed by incidents, pupil voice, staff confidence, technical changes and updates from EA/CPSS/C2k and recognised specialist organisations.

18. Monitoring, Records and Review

- The policy will be reviewed annually and sooner following significant guidance, technology or safeguarding changes, or a serious incident.
- The Principal, Designated Teacher and Online Safety/ICT Co-ordinator will review patterns in concerns while maintaining confidentiality.
- Pupil, parent and staff voice may inform curriculum and policy review.
- Governors will receive appropriate assurance information without unnecessary personal data.
- Related risk assessments, acceptable-use materials, consent records and incident procedures will be updated when this policy changes.

19. Linked School Policies

- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Pastoral Care & Positive Behaviour Policy
- Addressing Bullying Policy
- Data Protection Policy
- Complaints Procedure Policy
- Special Educational Needs Policy
- Educational Visits Policy

20. Key Guidance and Support

- Education Authority: Online Safety resource library
- Education Authority: Policies and Guidance for Schools
- Education Authority: Data Protection Guidance
- Safer Schools NI
- UK Safer Internet Centre
- CEOP Education
- SBNI Online Safety Hub
- PSNI: Keeping Children Safe Online
- Childline