Online Safety Policy

2025 – 2026

Reviewed by Mrs H Smith and Ms C Stewart December 2025

To be reviewed September 2026 or sooner if needed

The purpose of this policy statement is to:

- ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices

- provide staff and volunteers with the overarching principles that guide our approach to online safety

- ensure that, as an organisation, we operate in line with our values and within the law in terms of how we use online devices. The policy statement applies to all staff, volunteers, children and young people and anyone involved in Nateby Primary School's activities.

Technology affects all our lives and moves forward at a great pace. Nateby Primary school strives to teach and use ICT across the curriculum in interesting and creative ways. We teach the skills of ICT as well as helping children and the wider community to navigate the risks of using ICT.

Roles & Responsibilities

Governors: Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body / Board has taken on the role of E-Safety Governor. An E-Safety report will be provided at each Standards & Effectiveness meeting.

Headteacher: The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day-to-day responsibility for e-safety will be delegated to the E-Safety Subject Lead.

The Headteacher and (at least) another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Headteacher is responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

Online Safety Subject Lead: Nateby Primary School has a named member of staff who has a day-to-day responsibility for E- Safety. The role of the coordinator is;

- to take day to day responsibility for e-safety issues and have a leading role in establishing and reviewing the school e-safety policies / documents
- to ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place,
- to provide training and advice for staff, to liaise with school technical staff,

- to receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments,
- to provide reports for the relevant committee meetings.

Technical Staff: Nateby Primary School has a managed ICT service provided by an outside contractor, it is the responsibility of the school to ensure that the managed service provider carries out all the e-safety measures that would otherwise be the responsibility of the school technical staff.

Technical staff are responsible for:

- ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body E-Safety Policy / Guidance that may apply.
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant.
- that the use of the network / internet / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Coordinator for investigation.
- that monitoring software / systems are implemented and updated

Teaching & Support Staff: All teaching & support staff are responsible for ensuring that;

- they have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the E-Safety Coordinator for investigation
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the e-safety and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Safeguarding designated person: DSL and DDSL are trained in e-safety issues and are aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data

- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils: All pupils

- are responsible for using the *school* digital technology systems in accordance with the Pupil Acceptable Use Policy.
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the *school's* E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents & Carers: Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' workshops, newsletters, and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- use of Parent/ School Facebook page
-

Use of mobile phones and cameras

This section is applicable to Early Years Settings (3-5) under The Statutory Framework for EYFS requirements which come into force on 01.09.2012

"The safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff, and cover the use of mobile phones and cameras in the setting" EYFS 2012 s3.4.

Children have their photographs taken to provide evidence of their achievements for developmental records (The Early Years Foundation Stage, EYFS 2012). Whilst in school, staff, volunteers and students will use a school ipad to take photographs of children to be used in their evidence files. When on school trips, only school staff are allowed to use their mobile phone to take photos of the

children. These need to be transferred onto a school laptop and deleted from their phone on the same day.

Procedures

Under the Data Protection Act 1998, the school must seek parental consent to take photographs and use video recorders. Photographs will be stored on the 'R' Drive which is accessible by staff only. Each staff member has a password. Photographs will be deleted from the 'R' drive 2 years after the children have left Nateby School unless they are in a photo with other children in which case it will be deleted 2 years after those pupils have left year 6.

Photographs are to be kept on school laptops/ PCs and school network only. They may be printed off for use within school. All teaching staff have access to the 'R' drive where they are stored and printed from. At the beginning of each new academic year, permissions are sent out to parents asking which media platforms they give permission for their child's photograph to be used. A copy of this is displayed in the school office and placed inside each class register. As a double precaution, if photographs are to be used in other media or promotional material special permission from parents and guardians will be obtained prior to submission.

As set out in our Safeguarding policy, parents are NOT permitted to record children at a school event such as sports day, outings/trips, Christmas and fundraising events. Any recordings will be made by a member of school staff, or by a professional. The videos/recordings will be checked and approved by a member of school staff and then published on the school website or messaging platform. Children completing activities on residentials will be photographed by designated teachers who will use school equipment or their own phone. Photos will be uploaded onto the school website and messaging platform before being deleted from phones. A member of staff will check to make sure that photos are deleted from personal phones. Teachers will ensure that children are appropriately dressed and that photographs are only taken where children are part of an associated activity.

Staff and any other adult on school premises will only be permitted to use their mobile phones in their breaks. They should be left in the staffroom and should not be taken in to classrooms. Anyone expecting an urgent call that cannot be taken through the switchboard should leave the phone at the office for the bursar to answer on their behalf when they can then pass the call on. All staff can use the phones in school for urgent calls.

- **Cameras and mobile phones are prohibited in all toilet areas**

Use of digital media

- The school will seek consent from the parents/carers and members of staff at the start of each new school year for images of children/staff to be used for media purposes and the school website.
- The school will keep digital images of children for 2 years after as above they leave and may only be used if deemed appropriate. The images will be deleted after this time period.
- Staff and pupils are aware that full names and personal details will not be used on any digital media, particularly in association with photographs.

- Staff recognise and understand the risks associated with publishing personal images, particularly in relation to Social Network Sites.
- The school ensures that any photographs/videos are only stored in school on the 'R' drive, used only for school purposes and are only accessible to the appropriate staff/pupils.
- When taking photographs, staff will ensure children are appropriately dressed and not participating in activities that could be misinterpreted.
- Parents/carers will be permitted to use cameras to take photographs of their own child and others, ONLY with the permission of their parents. However, these images MUST NOT be broadcast or published online. This is outlined in the Parent's AUP.

Communication Technologies

Email/School Messaging Platform

- Staff and pupils only use the approved e-mail system as provided by Ed-It.
- Only official school email addresses should be used to contact staff/pupils.
- Any school related business will be done through school email accounts.
- Staff and pupils are aware of the risks of accessing content from external e-mail accounts and will keep any such access to a minimum.
- Staff are aware they must report any instances of SPAM on school's email accounts, to the schools technical support – Ed-It.
- Staff are aware that email is covered by The Data Protection Act (1988) and The freedom of Information Act (2000), meaning that safe practice should be followed in respect of record keeping and security.

Social Networks

- Pupils must not reveal personal details of themselves or others in an e-mail or arrange to meet anyone without specific permission.
- All users are aware that all email communications may be monitored at any time in accordance with the AUP.
- Staff and pupils must immediately report any email that makes them feel uncomfortable, is offensive, threatening or bullying in any nature.
- The school will block/filter access to social networking sites, except those specifically designed to support educationally approved practice.
- Pupils and parents will be advised that the use of social network sites outside of school is inappropriate for primary age pupils unless strictly supervised.
- Staff must not give personal contact details to pupils or parents/carers including mobile phone numbers or personal websites.
- Staff must not communicate with pupils using any digital technology where the communication may be deemed inappropriate.
- If staff choose to use a social networking site, details must not be shared with pupils or parents/carers and privacy settings set to a maximum.
- Staff will not add pupils or parents as 'friends' on any Social Network Site.

- Staff are made aware of the importance of conducting oneself in a professional manner if personal content is made available on the web.

Instant Messaging

- Staff and pupils will only use secure messaging, forum or chat systems within their Virtual Learning Environment.
- Staff and children are aware of the risks involved in using this technology e.g. viewing inappropriate images or making unsuitable contacts.

Virtual Learning Environment

Websites and other online publications

- The school website and its messaging platform, Weduc, communicates online safety messages to pupils, parents and carers.
- Staff and pupils are aware of the guidance for using digital media and personal details on the website (see Digital Images).
- The Head Teacher has overall responsibility for the content that appears on the school website.
- All staff have had the relevant training and are aware of the guidance for accessing, editing and updating the school website.
- Staff are aware that this content is available for everybody to see and are to follow the guidance for this. Staff are also aware of the guidance regarding personal information on the website (see also 'Use of Digital Media').
- Downloadable materials are in a read-only format where necessary, to prevent content being manipulated and potentially redistributed without the school's consent.

Misinformation & Disinformation

Nateby Primary school recognises that children may encounter misinformation (false information shared without intent to harm), disinformation (false information deliberately created or shared to mislead), and conspiracy theories (unfounded explanations that present events as secret plots) when using the internet and digital technologies. As part of our commitment to safeguarding and promoting critical thinking, we teach pupils age-appropriate skills to question the reliability of online content, check information using trusted sources, and understand how images, videos and messages can be edited, manipulated or taken out of context. Staff will support pupils in discussing online content safely and respectfully, helping them to distinguish between facts, opinions and beliefs. We will work in partnership with parents and carers to promote open conversations about online content at home and at school. Any content that may cause harm, distress, or promote unsafe or extremist views will be addressed promptly in line with our safeguarding and behaviour policies.

Acceptable User Policy

- Staff, pupils and parents/carers should all understand, agree to and sign their own AUP.

- Each AUP will be relevant to their setting and purpose and will be regularly communicated to all users, particularly when changes are made to either the online safety policy or the AUP.
- The AUPs will outline acceptable behaviour and use when using technologies, outline sanctions for its misuse and provide advice on reporting incidents.
- The AUP's will provide guidance on how to report any failings in technical safeguards.
- The AUPs will stress the importance of online safety education.

Dealing with incidents

- It is the responsibility of the Head Teacher/SLT/and the online safety Champion (Ms Stewart) to deal with online safety incidents.
- All staff are aware of the different types of online safety incident and how to respond appropriately i.e. who to inform.
- Pupils are aware of procedures in the event of an online safety incident and are reminded frequently during any lessons using the internet.
- Online Safety incidents are logged using CPOMS and all staff are aware of procedures for its use.
- School receives immediate reports from 'SurfProtect' of any suspicious or Prevent activity. The DSL and SLT monitor any reports and provide any further action if required.
- Incidents are monitored frequently by the online safety Champion and the Head Teacher is kept informed of any such incidents.
- Staff will contact the pupil's parents if an online safety incident has occurred in school or if continual misuse of technology is logged.
- All staff are aware of the procedures in place to protect staff in the case of a suspected incident/allegation involving a staff member.

Infrastructure and technology

Pupil access

- When using school equipment and accessing online materials, children will be supervised by a member of staff.

Passwords

- All staff and pupils from Year Two upwards have a secure username and password to use on the school network.
- Staff and pupil are reminded of keeping their passwords secure.
- Class teachers will have a copy of pupil's usernames and passwords.
- The Headteacher has access to the administrator password for the school network, however, the school ICT Technician updates the system with the direction of the Head Teacher.

Software/hardware

- The school buys licences for all software and abides by the specific user agreements for each software.
- The school has an up to date, on- line record of appropriate licences for software and the Head Teacher has responsibility for maintaining this.
- School ICT equipment and software is audited annually
- The school ICT technician installs updates for the system with the direction of the Head Teacher.

Managing the network and technical support

- All servers, wireless systems and cabling are securely located and physical access is restricted.
- All wireless devices have had their security enabled and are only accessible through a secure password.
- The School's ICT Technician is responsible for managing the security of the network with direction from the Head Teacher.
- The safety and security of the school network is reviewed on an annual basis.
- The school's systems are kept up to date in terms of security through the ICT Technician.
- Staff and pupils are required to log out of a school system when a computer is left unattended where 'Any Desk' is in use the computer screen must be switched off and the room itself must be locked
- Pupils are not permitted to download executable files or install software.
- Pupils are aware they must report any suspicion or evidence of a breach of security to their teacher who will then report to the headteacher who may discuss with the online safety Champion
- Staff are aware they must report any suspicion or evidence of a breach of security to the online safety Champion.
- Staff and pupils have clearly defined access rights to the school network and are aware of which drives they have access to on the network.
- Staff will only use school equipment e.g. laptops for school use.
- Staff are aware that network monitoring may take place by the Head Teacher.
- The school's external support providers (Ed-it) are aware of our school's standards and requirements regarding online safety.
- The Head Teacher is responsible for liaising with the technical support staff.

Filtering and virus protection

- The school's filtering is managed by Ed-it
- SurfProtect provides the HT and bursar with immediate notifications of any suspicious activity.
- As part of the Safeguarding procedure, the SLT conduct their own 'test' to ensure the filtering system is working.
- Staff are aware of the procedures for reporting suspected or actual virus infection.

- Staff, pupils and visitors are made aware that monitoring systems are in place when using the internet.

Education and Training

Online safety across the curriculum

- Staff provide pupils with regular, planned online safety teaching within a range of curriculum areas, including online safety assemblies and explicitly as part of the ICT curriculum.
- Staff will provide an extra focus on online safety during the National online safety Awareness Week.
- Individual teachers will differentiate the online safety curriculum as appropriate for any children with special educational needs.
- Key stage 2 pupils are made aware of the impact of Cyberbullying through the online safety and PSHE curriculum.
- Key stage 2 pupils will be taught to evaluate the content of online materials and develop good research skills across the curriculum.
- Staff will continually promote the importance of the AUP and will encourage pupils to adopt safe and responsible use of ICT both within and outside school.
- Pupils are reminded of safe internet use through classroom displays and safety rules.

Online safety- Raising Staff Awareness

- All staff have received advice and guidance on online safety training by the Headteacher or a lead professional and are aware of their responsibilities as outlined in the school policy.
- The online safety Champion will provide advice and guidance on online safety training to individuals as and when required e.g. Student Teachers.
- Through online safety training, staff are made aware of the issues which may affect their own personal safeguarding e.g. use of Social Network Sites (also outlined in Social Networks).
- All staff will promote and model responsible use of ICT and digital resources.
- Regular updates on the online safety policy, AUP and general online safety issues are discussed in staff meetings.

Online safety- Raising parents/carers awareness

- Parents are made aware of the issues of online safety through online safety awareness sessions and also through the promotion of external online safety resources/online materials. This is published on the schools messaging platform, Weduc, and in the newsletter.
- A monthly online safety newsletter is sent out to parents and posted on the school website and school messaging platform.

Online safety-Raising Governor's awareness

- School Governors are made aware of online safety through updates and discussions at Governor's meetings and also staff/parent meetings.

- A monthly online safety newsletter is sent out to governors and posted on the school website and newsletter
- The online safety policy will be regularly reviewed and approved by the governing body.

Appendices

In this school there is strict monitoring and application of the Online Safety Policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely a need to apply sanctions

• All members of the school community will be informed about the procedure for reporting online safety concerns (such as breaches of filtering, cyber-bullying, illegal content etc.).

• The Headteacher will record all reported incidents and actions taken in the School Online Safety incident log and other in any relevant areas e.g. Bullying or Child protection log.

• The Designated Safeguarding Lead (Headteacher) and DDSL will be informed of any online safety incidents involving Child Protection concerns, which will then be escalated appropriately – See Child Protection Policy and procedures for dealing with concerns.

• The school will manage Online Safety incidents in accordance with the school discipline/behaviour policy where appropriate.

• The school will inform parents of any incidents of concerns as and when required.

• After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required.

• Where there is cause for concern or fear that illegal activity has taken place or is taking place then the school will contact the Safeguarding Hub and escalate the concern to the Police.

• If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Safeguarding Hub – see Child Protection Policy and procedures.

Pupils- infringements and sanctions:

Incidents:									