



Nateby Primary School

Online Safety Policy

2022

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 Coordinator.

- 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 Coordinator: 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.
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- 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: SDP and Deputy SDP 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). Staff, visitors, volunteers and students are not permitted to use their own mobile phones to take or record any images of children for their own records during session times.

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. They will be deleted from the memory card termly after being up-loaded to the 'R' drive.

The school's digital camera/s or memory cards must not leave the school setting unless on an official school trip. Photos are printed/ uploaded in the setting by staff within 1 term and once done images are then immediately removed from the camera's memory.

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. They may be displayed on the school website and may have other children in the background. If they are used in other media or promotional material special permission from parents and guardians will be obtained prior to submission.

Parents are permitted to record children generally at a school event such as sports day, outings/trips, Christmas and fundraising events. They must record children in whole groups unless the child is their own or they have the parents' permission at the time. Children completing activities on residential will be photographed by designated teachers who will use school equipment and will up-load photographs to school CDs for parents. 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**
- **It is unacceptable for teaching staff to use personal mobile phones for school trips.**

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. Parents are made aware of this time scale.
- 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.
- Staff will use school equipment to take photographs/videos they may not use personal equipment.
- The school ensures that any photographs/videos are only stored in school on the 'T' 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 and videos in school but must not broadcast or publish them publically online. This is outlined in the Parent's AUP.

Communication Technologies

Email

- Staff and pupils only use the approved e-mail system as provided by the Lancashire grid for Learning.
- 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 Westfield Centre.
- 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 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 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.

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 and the online safety Champion (Mrs Gallagher) 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 in a digital 'log book' and all staff are aware of procedures for its use.
- 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 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 every 3 years or earlier if necessary
- 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 only 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 use encrypted removable storage devices for storing work to be taken home.
- 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
- Staff are aware of the procedures for reporting suspected or actual virus infection.

Education and Training

Online safety across the curriculum

- Staff provide pupils with regular, planned online safety teaching within a range of curriculum areas, using the Lancashire ICT Progression document.
- 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 online safety Champion 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.
- The online safety champion has received external training from the local authority on the most up to date information.
- 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.

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.
- The online safety policy will be regularly reviewed and approved by the governing body.

Prevent

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. As a school, we ensure that suitable filtering is in place. More generally, as a school we have an important role to play in equipping children and young people to stay safe online, both in school and outside. As highlighted in KCSiE (Sept 2022) Children are vulnerable to extremist ideology and radicalisation. Similar to protecting children from other forms of harms and abuse, protecting children from this risk should be a part of a schools' safeguarding approach.

Extremism is the vocal or active opposition to our fundamental values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. This also includes calling for the death of members of the armed forces.

Radicalisation refers to the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

Terrorism is an action that endangers or causes serious violence to a person/people; causes serious damage to property; or seriously interferes or disrupts an electronic system. The use or threat must be designed to influence the government or to intimidate the public and is made for the purposes of advancing a political, religious, or ideological cause.

Online safeguarding is integral to our school's computing curriculum and is also embedded in PSHE. General advice and resources for schools about online safeguarding are available on the UK Safer Internet Centre website. As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups. As highlighted in The Prevent Duty-June 2015 we must provide an environment which protects and educates our children to have "due regard to the need to prevent people from being drawn into terrorism under the PREVENT duty by identifying children who may be vulnerable to radicalisation and know what to do when they are identified". We educate our children to build their resilience to radicalisation by promoting fundamental British Values and enabling them to challenge extremist views. It is important to emphasise that the Prevent duty is not intended to stop pupils debating controversial issues but provide a safe open space in which pupils and staff can understand the risks associated with terrorism.

Reviewed by Mrs C Vardey and Mrs L Gallagher February 2021

To be reviewed February 2024 or sooner if needed

Reviewed by Mrs Vardey 09.11.22