Morpeth First School
Online Safety policy

Headteacher – Mrs N Fielding
Designated Safeguarding Leads - Sandra Bell, Nadine Fielding
Chair of Governors – Mr C Appleby
Safeguarding Governors (Including Online safety) – Craig Appleby, Nicola Darrington
Technician – Mr D Matthewson
Computing Subject leader – Mr E Jefferson
Filtering and monitoring systems supplied by Northumberland County Council

Date of Policy - September 2023

Reviews

Date	Reason for review	Updates/changes	Completed by
Sep 24	Annual review	Updated wording/ definition of 4C's (p2) Updated Chair of Govs (p1)	SBell E Jefferson

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

At Morpeth First School, we recognise that Online safety does not stand alone, but is part of the ethos of safeguarding which exists in the school. As such, it is to be overseen by the Designated Safeguarding Leads who have the overall responsibility for safeguarding and child protection in the school in line with Keeping Children Safe in Education 2023.

However, all staff have a duty of care towards pupils and everyone in school has a responsibility to ensure that any incidents involving breaches of online safety are reported to the DSL's and are regarded as safeguarding concerns.

The school Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy
- is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school, and how they should use this understanding to help safeguard learners in the digital world.

Online Safety encompasses the use of new technologies, internet and electronic communications, such as mobile phones, collaboration tools, and personal publishing.

Keeping Children Safe in Education categorises online safety into four groups:

- **Content**- includes the range of digital material, entertainment and media found online, including websites, apps, games and social media.Although much of this content is beneficial, there exists content that is material which is misleading, inappropriate or harmful.

- **Contact** -this refers to online interactions and connections between individuals. Some of these may be harmful including those with online predators or exposure to inappropriate content through peer pressure.
- **Conduct** - this focuses on the behaviour of children and young people online with the anonymity of the internet sometimes leading to negative behaviours
- **Commerce** - this relates to the commercial aspects of the internet world with advertising, online shopping in app purchases and the risks of online gambling and scams.

Our online safety policy aims to support children in navigating these 'four C's' of online safety, supporting them to critically evaluate online content, encouraging healthy digital relationships and communications; encouraging the use of positive online behaviour and highlighting the significance of protecting personal and financial information. We will endeavour to pinpoint critical online safety risks and equip children and young people with the knowledge to identify and manage these risks effectively at an age appropriate level.

The school's Online safety policy will operate in conjunction with other policies including;

- Safeguarding and Child Protection
- PSHE
- Anti bullying
- Behaviour
- Curriculum
- Data Protection
- Photography
- Preventing extremism and radicalisation
- Social networking policy and guidance
- Acceptable use policy
- Staff Code of Conduct

as well as statutory Government guidance including 'Keeping Children Safe in Education' and 'Working Together to Safeguard Children'.

Online Safety relies on effective practice at a number of levels;

- Responsible ICT use by all staff and students, encouraged by education and made explicit through published policies.

- Sound implementation of online safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband including the effective management of filtering and monitoring of content and use.
- The appointment of an online safety governor
- The support of the head teacher, SLT and governing body
- Supporting parents in the use of ICT and emerging technologies at home.

1. Introduction

The purpose of this policy is to;

- Establish the ground rules that are in place in Morpeth First School for using the internet and electronic communications, such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate the pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- Describe how these fit into the wider context of our discipline and PSHE policies.
- Demonstrate the methods used to protect children from accessing sites containing inappropriate material such as pornography, racist or politically extreme views, and violence.
- To be reviewed regularly and in the light of new technologies or concerns arising from day to day use. This will be carried out with the involvement of staff, pupils, governors and parents

2. The Role of the DSL

- To be responsible for regularly monitoring internet and device use and updates the head teacher, governors and senior managers on a regular basis
- To act as a point of contact for online safety issues within the school
- To support the National Online Safety Strategy and disseminate up to date information among the staff and arranges staff development as a result of information regarding emerging and changing technologies
- To be responsible for the duty of care requirements under the safeguarding arrangement within the school
- The DSL is supported in this role by the Safeguarding governors

3. **Role of the filtering and monitoring provider (NCC)**
    - Oversee the day to day management of filtering and monitoring systems in line with the school's requests
    - Provide training and support for the DSL in using the systems
    - Provide reports to the school
    - Complete actions following reports by the school.

4. **The role and responsibilities of the SLT/ Govs**

    - The overall responsibility for meeting the digital and technology standards specified HERE
    - The production/review/monitoring of the school Online Safety Policy/documents
    - Procuring adequate filtering and monitoring systems for the school
    - Responsibility for requests for filtering changes
    - Mapping and reviewing the online safety education provision – ensuring relevance, breadth and progression and coverage
    - Monitoring and reviewing network/filtering/monitoring/incident logs, where possible
    - Encouraging the contribution of learners to staff awareness, emerging trends, and the school online safety provision
    - Consulting stakeholders – including staff/parents/carers about the online safety provision
    - Ensuring the provision of up to date online safety and safeguarding training

5. **The role and responsibilities of staff**
    - Staff are expected to follow the acceptable use policy and staff code of conduct at all times
    - Staff are responsible for monitoring 'in person' what children are accessing and provide effective supervision at all time when children access digital devices
    - Staff are expected to take part in online safety training as part of their safeguarding responsibilities
    - Staff are expected to report any concerns or breaches of online safety, either witnessed or suspected
    - Staff are trained in the use of new technologies including any associated possible safety issues as they arise
    - Staff are asked to report any 'overblocking' to the DSL. This will be reviewed and logged by the SLT.

6. Teaching and Learning

- The internet is an essential element in 21st century life for business and social interaction. The school has a duty to provide children and staff with quality internet access as part of the learning experience.
- Internet access is part of the statutory curriculum and a necessary tool for students and staff.
- The school's curriculum internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils through the installation of Fortinet filtering software. This is managed by Northumberland County Council as part of the Service Level Agreement (See below).
- Pupils are taught about acceptable internet use and are given clear objectives for internet use.
- As part of each year group's curriculum, pupils will be taught all areas of online safety through the teaching of each curriculum area.
- Pupils are expected to acknowledge and agree to the acceptable use policy when logging onto the curriculum system with their individual passwords.
- Pupils are taught about effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school ensures that the use of the internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils are taught what to do if they come across or receive offensive or unpleasant material whilst using technologies through reporting to teachers/parents, or using the 'report' button on internet sites at home.
- Staff receive annual training online safety issues as part of the safeguarding training package or at induction.
- Staff are aware of how to report instances of unsuitable material using the online safety incident guidelines provided by NCC.

7. **Responsibilities of Parents and Carers**

The school will make every effort to help parents/carers understand some of the issues involved in this through:

- Publishing the school's online safety policy on the website
- Provide them with a copy of the pupil acceptable use agreement
- Providing information on a termly basis about matters around online safety on personal devices in the home as well as national initiatives

8. Using Technologies

Internet Access - filtering and monitoring systems

The school's ICT curriculum system is filtered through Fortinet filtering software, and monitored by SENSO through the Northumberland County Council Service Level Agreement. Both of these systems comply with standards specified by the DfE and Internet Watch Foundation and provide the device, IP address and individual, the time and date accessed and the search term monitored or blocked.

- Fortinet blocks certain categories of content, such as adult content, gambling etc, specific bundles of programs related to e.g. Social media platforms and individual websites. From time to time, it may be necessary to block or unblock certain websites which are requested via NCC ICT support. Any change to group access or content being blocked or unblocked is noted by the DSL, and the reasons for this decision given.
- SENSO software monitors the use of the devices by identifying specific categories of words and records the user, the device and the time that this has occurred. A weekly report is sent to the DSL regarding unacceptable use of the system. This identifies individual pupils, staff or computers which have been used and reports on the types of inappropriate access. This can then be managed according to the school's behaviour policy or staff disciplinary procedures. Reports can be used to identify patterns or trends, for example, particular users or particular times of the day.
- Internet usage is also monitored by the class teacher supervising the lesson.

- Mobile devices (i-pads) have Local Authority recommended firewalls installed on them which are regularly updated if the internet is accessible on the devices.
- Virus protection is updated regularly by the ICT Technician.
- Staff are not permitted to access the school's wireless technology with their personal laptops unless SENSO is installed.
- Staff using school laptops at home are aware that Senso is installed on all units and that the appropriate use of the equipment will be monitored when the laptop accesses the school's wireless system on its return to school.

Systems are reviewed and reported on at least once per term to ensure that they are fit for purpose and nothing has been changed or deactivated without prior knowledge. This may also be carried out when there is a known safeguarding or security breach, or a change in working practice. . Responsibility for testing this lies with the Governing body, the SLT and the DSL. A report of the findings should include:

- when the review was undertaken
- who reviewed the system
- what was tested or checked
- The resulting actions

Testing for child sexual abuse content, unlawful terrorist content and adult content can be done through the SWGfL testing tool HERE.

E-Mail

- Pupils may only use approved e-mail accounts on the school system where available (e.g. School 360).
- Pupils must immediately tell a teacher if they receive offensive material or comments via e-mail.
- Pupils are taught not to reveal personal details of themselves or others in electronic communication, or arrange to meet anyone.
- E-Mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper.
- Staff should, wherever possible, use the admin email address for contacting parents. Personal or NCC e-mail addresses should not be used to contact parents without discussing the implications of this with theDSL/headteacher. If parents make contact through the county email system, this should be reported to the DSL/Head Teacher.

- Under no circumstances should staff issue personal or work email addresses to pupils or contact pupils.
- Live streaming is not permitted.

School Website

- The contact details on any school website should be the school address, e-mail and telephone number. Staff and pupil details or personal information is not to be published.
- The head teacher has overall editorial responsibility and ensures that the content is accurate and appropriate.
- Photographs that include pupils are selected carefully so that they do not enable individual children to be clearly identified
- Pupil's full names are not used anywhere on the website
- Written permission from parents/carers must be obtained before photographs of pupils are published on the website. This is done on an annual basis for that academic year. Any parent who wishes to withdraw this permission should contact the school office.
- Photos being used for any purpose outside the school (press or website) should be checked by a second member of staff to ensure that parental permission is being adhered to.

Social networking and personal publishing

- Any social network sites used to support learning or links with other schools must be secure. They must be approved by the Head Teacher before use and any content uploaded should be checked by the teacher. The teacher is also responsible for pre checking any content to be viewed by the children .
- The school blocks access to public social networking sites . Newsgroups are also blocked.
- Pupils are told never to give information which may allow them to be identified.
- Parents are kept up to date on online safety matters through a termly newsletter and information and links on the website.
- Parents are given the opportunity to suggest training or information requirements that they may have regarding online safety.

- Staff are provided with guidance to support their safe use of social networking sites out of school through the Staff Social Network policy and County Council Guidelines.

Mobile Phones and Mobile Devices

- In order to ensure the safety of both children and staff, mobile phones and other mobile devices should not be visible in the vicinity of children during the school day.
- Mobile phones should not be used during teaching sessions. If it is felt necessary to make phone calls/take messages during the school day this must occur during lunch / break times in an area where there are no children (e.g. empty classroom/staff room). This is to safeguard teachers as well as pupils.
- Staff should, wherever possible, use the school mobile phones when off site.
- Staff should not give out personal mobile numbers to pupils or parents. If parents contact staff via their personal phone number, this should be reported to the DSL/Head Teacher.
- Pupils are not permitted to bring mobile phones and other devices with photographic / video/messaging capability (e.g. smart watches) into school except with the express permission of the head teacher / senior staff. This technology is not permitted on trips either.
- Pupils are not allowed mobile phones in school except in exceptional, previously agreed circumstances (e.g. where a child is going between separated parents) and this will be on the understanding that the phones will not be turned on while on the school premises, are kept by the teacher in a safe place. and are brought in at the owners risk. Infringement of these rules will result in the phone being confiscated for the duration of the school day and parents contacted.
- As part of the children's online safety education, children are taught how to respond in the instance of receiving malicious messages or texts.

Photographs

- Photographs/videos taken during school trips should only be taken by staff members on cameras/i-pods which are directly downloaded into the appropriate folder on the school network. Any photographs taken on staff's personal cameras should be deleted as soon as they have been downloaded.

- If pupils use the school cameras/i-pods, the teacher responsible for the group should supervise the shot where possible.
- Parent volunteers on trips are instructed that they are not allowed to take photographs on their mobile phones.
- All photographs taken by children and staff should be scrutinised by the teacher for suitability before being used for any purpose.
- All photographs / videos should be viewed by the teacher for appropriateness before publishing openly. Photographs which may cause the subject to be embarrassed or upset should be deleted. Any child taking photographs deemed to be inappropriate should be dealt with in terms of the behaviour or bullying policy as appropriate.

9. Managing Technologies

Emerging technologies are evolving at a rapid rate and although every attempt is made to protect children from offensive or inappropriate material and misuse, there may be occasions when inadvertent access occurs. There may also be situations where access is deemed to be 'overblocked' and therefore impose unnecessary restrictions on teaching and learning. The following points apply;

- The filtering system will be 'tested' to ensure that it complies with the requirements once a term. This will be the overarching responsibility of the DSL and the online safety governors with the support of the ICT technician if necessary. A report will be completed each time this is done.
- If staff or pupils discover an unsuitable site, it must be reported immediately to the teacher and then the DSL, who will report the site to the appropriate person in the Local authority according to the safety incident flow chart displayed in the staff room. Following the flow chart, if it is felt that the incident is a child protection issue it will be dealt with by the DSL.
- If staff feel that they cannot access sites which would be useful for teaching and learning, they should contact the DSL who will make a decision with the SLT on whether a request should be made for the site/s to be unblocked. This will be noted with reasons provided for the decision.
- If an incident involves extremist material, the police should also be notified as well as the NCASP if it is felt that the access has been deliberately sought

- All internet access including e-mails will be monitored through SENSO on the curriculum network. The admin system is protected by a separate firewall system.
- Regular updates from the Local Authority providing guidance for the safe use of technologies is acted on as it is received.

10. Policy Decisions

- All staff and pupils must agree to the acceptable use policy in ICT agreement which forms part of the staff induction process and on the desktop screen following the login procedure.
- The AUP is regularly explained to the children at their level to ensure their understanding.
- The AUP is sent home each September and is available on the school website to ensure that parents are aware of the high priority that the school places on safe use of technologies. It is also displayed in areas where computers are present
- SENSO reports are regularly monitored by the DSL, who in turn reports to the senior leadership team and the governors.
- The school keeps a record of all staff and pupils who are granted internet access.
- At Key Stage 1 / Early Years, access to the internet will be by adult demonstration with directly supervised access to approved online materials
- At KS2, access to the internet will be by supervised access to online materials filtered by Fortinet and monitored by SENSO

Assessing Risks

- The school takes all reasonable precautions to ensure that users access only appropriate material through the use of filtering and monitoring systems. Supervised access is recommended as the school is aware that no firewall system is completely infallible.
- The school audits and reports on ICT provision on a termly basis, or when new technologies are introduced to establish if the online safety policy is adequate and that its implementation is effective.

Dealing with Online Safety reports

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The Designated Safeguarding Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures.
- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the local authority.
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.
- All incidents should be logged and a note made of the actions taken and the reasons for this.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.
- The DSL will inform class teachers if it is felt that there has been an infringement of the AUP by a child in the class. Minor infringements will first result in a warning given to the child. Further or more serious infringements will be dealt with under the school's behaviour policy.
- Any infringement of the school policy by pupils or staff which is deemed to be a child protection issue will immediately be reported to the appropriate authorities via the flow chart system (see appendix). Where this involves a member of staff, disciplinary procedures will be instigated.
- Incidents where staff or pupils are suspected of having obscene images on a mobile device, will be dealt with via the flow chart system and via the disciplinary procedures.

- Learning from the incident (or pattern of incidents) will be provided anonymously to:
  - Members of the SLT and safeguarding governors
  - Staff to update on potential hazards
  - Learners where appropriate
  - Parents/carers through newsletters/website as appropriate
  - Local authority as appropriate

Next Review date September 2025 (or sooner if legislation or incidents require it)

Appendix A

Termly Testing

Date of test _____

Staff involved in Review

	Child Test login	Adult test login	Comments / Actions
Can adult material be accessed? Y/N			
Can terrorist material be accessed?			
Can gambling sites be accessed?			
Have mobile devices/apps been checked for above?			
Social media? (eg facebook twitter)			
Are monitoring red flags picked up on SENSO			

Signed DSL _____

Appendix B

Flowchart when dealing with online safety incidents