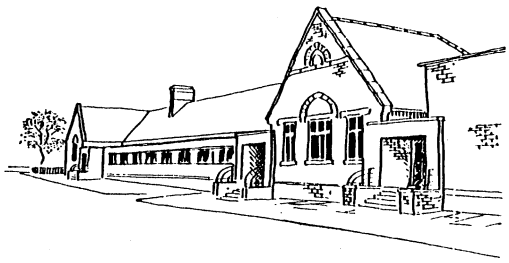
Mundella Primary School Policies



Online Safety Policy

Date Created/Updated: Nov 2019

Responsibility: Headteacher

Date to be reviewed: Nov 2022

Online Safety Co-ordinator: Will Smith, Headteacher
Online Safety Governor : Ellen Oldham-Hepper

This Online Safety policy is to ensure everyone has the chance to develop a set of safe and responsible behaviours that will enable them to reduce the risks whilst continuing to benefit from the opportunities that are available from using the Internet and new technologies. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put users at risk; these risks can be categorised into three main areas:

Content: being exposed to illegal, inappropriate or harmful material
Contact: being subjected to harmful online interaction with other users
Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

We aim always to keep our pupils safe whilst encouraging them to meet their full potential.

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, work placement students, visitors) who have access to and are users of school ICT systems, both in and out of school.
The school will identify within this policy how incidents will be managed and will, where appropriate, inform parents/carers of incidents of inappropriate online safety behaviour that takes place.

The Education Act 2011 gives the school the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully or harass others.

Keeping Children Safe In Education September 2019 This is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Education (Non-Maintained Special Schools) (England) Regulations 2011. Schools and colleges must have regard to it when carrying out their duties to safeguard and promote the welfare of children. The document contains information on what schools and colleges should do and sets

out the legal duties with which schools and colleges must comply. It should be read alongside statutory guidance **Working Together to Safeguard Children**.

Communication of the Policy:

- The senior leadership team will be responsible for ensuring all members of school staff and pupils are aware of the existence and contents of the school Online Safety policy and the use of any new technology within school.
- The Online Safety policy will be provided to and discussed with all members of staff formally.
- All amendments will be published and awareness sessions will be held for all members of the school community.
- Any amendments will be discussed by the School Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- The Online safety curriculum will be taught throughout the year in all year groups, linking closely with the computing and PSHE curricula.
- The key messages contained within the Online Safety policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed Online Safety messages across the curriculum whenever the internet or related technologies are used
- The Online Safety AUP will be introduced to the pupils at the start of each school year
- Safeguarding posters will be prominently displayed around the school

We believe that Online Safety is the responsibility of the whole community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Headteacher / DSL / Online Safety Co-ordinator

- The Headteacher has overall responsibility for Online safeguarding all members of the school community, though the day to day responsibility for the Online Safety curriculum will be delegated to the Online Safety Team.
- The headteacher and senior leadership team are responsible for ensuring that the Online Safety Team and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues when necessary.
- To be the first point of contact in school on all Online Safeguarding matters.
- The Headteacher and senior leadership team should ensure that they, and all other members of staff, are aware of procedures to be followed in the event of a serious Online Safety incident.
- To take day-to-day responsibility for Online Safeguarding within school and to have a leading role in establishing and reviewing the school Online Safeguarding policies and procedures.
- Receive and regularly review Online Safety incident logs and be aware of the procedure to be followed should an Online Safety incident occur in school.
- Create and maintain Online Safety Policies and procedures

Responsibilities of Senior Leadership Team:

- The Headteacher and senior leadership team are responsible for ensuring that the Online Safety Team and other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues when necessary.
- The Headteacher and senior leadership team should ensure that they, and all other members of staff, are aware of procedures to be followed in the event of a serious Online Safety incident.

Responsibilities of Online Safety Team:

- Develop and promote an Online Safety culture within the community
- To ensure that the school has an Online Safety curriculum and to ensure that this is not solely delivered in Computing.
- Make appropriate resources, training and support available to members of the school to ensure they are able to carry out their roles with regard to Online Safety effectively.
- Develop an understanding of current Online Safety issues, guidance and appropriate legislation
- To ensure that school Acceptable Use Policies are appropriate for the intended audience.
- Ensure that Online Safety is promoted to parents and carers
- Liaise with the LA, Safeguarding Sheffield Children Board and other relevant agencies as appropriate.
- To communicate regularly with school technical staff
- To ensure that the school Online safeguarding policy is systematically reviewed at agreed time intervals.
- To promote to all members of the school community the safe use of the internet and any technologies deployed within school.

Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's Online Safety policies and guidance
- Photographs of children and their full names should not appear together at any time.
- Digital images, video and sound will usually only be created using equipment provided by the school. However, on some occasions, (eg school visits, sports competitions, assemblies) photos may be taken with staff's own equipment. However, such pictures will be downloaded as quickly as possible onto school equipment and deleted from personal equipment.
- Read, understand and adhere to the school staff Acceptable Use Policy. (AUP)
- Be aware of what to do if an Online Safety incident occurs.
- Develop and maintain an awareness of current Online Safety issues and guidance.
- Model safe and responsible behaviours in your own use of technology.
- Embed Online Safety messages in learning activities where appropriate.
- Supervise pupils carefully when engaged in learning activities involving technology.
- Maintain a professional level of conduct in their personal use of technology at all times.
- To report any suspected misuse or problem to the Online Safety coordinator.

Responsibilities of ICT Technicians

- To read, understand, contribute to and help promote the school's Online Safety policies and guidance.
- To read, understand and adhere to the school staff Acceptable Use Policy.
- To report any Online Safety related issues that come to your attention to the Online Safety coordinator.
- To develop and maintain an awareness of current Online Safety issues, legislation and guidance relevant to their work.
- To maintain a professional level of conduct in your personal use of technology at all times.
- To support the school in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the school network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the school ICT system.
- To liaise with the local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on school-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within school.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to school-owned software assets is restricted.

Responsibilities of Pupils

- Read, understand and adhere to the school's pupil AUP
- Help and support the school in creating Online Safety policies and practices; and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for their own and others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
- Ensure they respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
- Understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if they know of someone who this is happening to.
- Discuss Online Safety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support your school in promoting Online Safety.
- Read, understand and promote the school pupil AUP with your children.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss Online Safety concerns with their own children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in your own use of technology.
- Consult with the school if they have any concerns about their children's use of technology.

Responsibilities of Governing Body

- Read, understand, contribute to and help promote the school's Online Safety policies and guidance.
- Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
- Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the Online Safety Co-ordinator in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in Online Safety activities.
- Ensure appropriate funding and resources are available for the school to implement their Online Safety strategy.

Learning and Teaching

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.

- We will provide Online Safety curriculum lessons in every year group, taught throughout the year, using the Sheffield Online Safety Curriculum.
- We will celebrate and promote Online Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant Online Safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.

- We will remind pupils about their responsibilities through the AUP which children sign at the beginning of every academic year.
- Staff will model safe and responsible behaviour in their own use of technology during lessons
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Students / Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.

How parents and carers will be involved

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:

- include useful links and advice on Online Safety occasionally in newsletters and on our school website
- include a section on Online Safety in the School Prospectus

Managing ICT systems and Access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Laptops will be "locked down" when the user is out of the room
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
- The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
- All members of staff will sign an end-user Acceptable Use Policy (AUP) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
- All pupils will discuss an age appropriate AUP and agree to follow these rules.
- At KS1 pupils will access the Internet using a class log-on, which the teacher supervises. All Internet access will be by working alongside a member of staff, or if working independently a member of staff will supervise at all times.
- At KS2 pupils will access the Internet using an individual log-on, which they will keep secure. Internet access will be supervised by a member of staff.
- Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet and/or server through their log-on. They will abide by the school AUP at all times.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. head teacher and member of technical support/SLT

- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to unsuitable material will never occur.
- The school will regularly audit ICT use to establish if the Online Safety policy is adequate and that the implementation of the Online Safety policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.

Filtering Internet access

- The school uses a filtered Internet service. The filtering is provided through YHGfL
- The school will always be proactive regarding the nature of content which can be viewed, sent or received through the school's internet provision.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Online Safety coordinator.
- If users discover a website with potentially illegal content, this should be reported immediately to the Online Safety coordinator. The school will report this to appropriate agencies including the filtering provider, LA, CEOP or IWF.
- The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Using email

- Pupils can only use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system could be monitored and checked.
- Staff should use approved email accounts when contacting external people. Personal email may be used for communicating with other staff.
- Pupils will be reminded when using e-mail about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using images, video and sound

The development of digital imaging technologies has created significant benefits to teaching and learning, allowing staff and pupils instant use of images that they have uploaded themselves or downloaded from the internet. However, everyone needs to be aware of the potential risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

- We will remind pupils of safe and responsible behaviours when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
- Digital images, video and sound will usually only be created using equipment provided by the school. However, on some occasions, (eg school visits, sports competitions, assemblies) photos may be taken with staff's own equipment. However, such pictures will

be downloaded as quickly as possible onto school equipment and deleted from personal equipment.

- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either with resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved.
- If pupils are involved, relevant parental permission will also be sought before resources are published online.

Using blogs. Wikis, podcasts and other ways for pupils to publish content online

We may use blogs/wikis/podcasts/other ways to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

- Blogging, podcasting and other publishing of online content by pupils will take place within the school learning platform or on recommended blog sites which require passwords. (eg Word Press) Pupils will not be allowed to post or create content on sites where members of the public have access such that the latter can add content.
- Pupils will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them. Pupils will not use their real name when creating such resources. They will be encouraged to create an **appropriate** "nickname."
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, social networking sites and other online publishing outside of school.

Using mobile phones

See also separate Mobile Phone policy

- Personal mobile phones will only be used during lessons with permission from the teacher.
- Pupils will be allowed to use their mobile phones for specific learning activities under the supervision of a member of staff.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a school mobile phone should be provided and used. If personal phones have to be used, the digits 141 should be placed in front of the number dialled as this makes the caller unidentifiable.
- Staff will not normally be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parents. However, some members of staff are members of the local community and so are personal friends of some parents. In these cases, mobile contact would be acceptable.

Mobile phones are a common vehicle for cyberbullying, through the recording of inappropriate images or video, distributing such images and videos via Bluetooth or other wireless technologies, or the sending of abusive text messages or via social media. At Mundella we regularly remind children of the unacceptability of this. (Please also see our Anti-Bullying Policy.)

Using new technologies

- As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an Online Safety point of view.
- We will regularly amend the Online Safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an Online Safety risk.

Protecting personal data

- We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Staff will ensure they properly log-off from a computer terminal after accessing personal data.
- Staff will not remove personal or sensitive data from the school premises without permission of the headteacher, and without ensuring such data is kept secure.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
  - The data must be encrypted and password protected
  - The device must be password protected
  - The data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.
- Staff and pupils will not leave personal and sensitive printed documents on printers within public areas of the school.

The school website and other online content published by the school

- The school website will not include the personal details, including individual e-mail addresses of staff or pupils.
- A generic contact e-mail address will be used for all enquiries received through the school website.
- All content included on the school website will be approved by the Computing Subject Leader before publication.
- The content of the website will be composed in such a way that individual pupils cannot be clearly identified.
- Staff and pupils should not post school-related content on any external website without seeking permission first.

Learning technologies in school

The grid below shows which technologies we have agreed as a staff will be allowed in school

	Pupils	Staff
	Pupils allowed Pupils allowed at certain times Pupils allowed with permission Pupils allowed with supervision Pupils not allowed	Staff allowed Staff allowed at certain times Allowed for selected staff Staff not allowed
Personal mobile phones brought into school	Pupils allowed to bring to school but must be handed in to teacher until end of day	Staff allowed
Mobile phones used outside of lessons	Pupils not allowed	Staff allowed
Taking photographs or videos on personal equipment	Pupils allowed at certain times eg school visits; projects	Staff allowed at certain times. Any items will be deleted as soon as possible
Taking photographs or videos on school devices (I-pad during lesson time for twitter and school mobile on school trips.)	Pupils allowed with permission	Staff allowed
Use of hand-held devices such as PDAs, MP3 players or personal consoles	Pupils allowed with permission	Staff allowed
Use of personal email addresses in school	Pupils not allowed	Staff allowed at certain times
Use of online chat rooms	Pupils not allowed	Staff not allowed
Use of instant messaging services	Pupils not allowed	Staff allowed under certain circumstances eg using Google mail instant messaging between professionals
Use of blogs, wikis, podcasts	Pupils allowed with supervision	Staff allowed
Use of video conferencing or other online video meetings	N/A currently	N/A currently

Dealing with Online Safety incidents

The following incidents may occur:

- accessing illegal content deliberately
- accessing inappropriate content deliberately
- accessing illegal content accidentally and failing to report this
- accessing inappropriate content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at school
- accessing social networking sites, chat sites, instant messaging accounts or personal email where not allowed
- accessing other non-educational websites (e.g. gaming or shopping websites) during lesson time
- downloading or uploading files where not allowed
- sharing your username and password with others
- accessing school ICT systems with someone else's username and password
- opening, altering, deleting or otherwise accessing files or data belonging to someone else
- using school or personal equipment to send a message, or create content, that is offensive or bullying in nature
- attempting to circumvent school filtering, monitoring or other security systems
- sending messages, or creating content, that could bring the school into disrepute
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- use of online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content)

Any incidents which occur should be reported to the Headteacher and will be dealt with appropriately. (See 'Response to an Incident of Concern')

There may be incidents where Staff contravene the expectations eg

- transferring personal data insecurely
- using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or communicating via social networking sites)
- failure to abide by copyright of licencing agreements (for instance, using online resources in lessons where permission is not given)

Incidents of this kind would be investigated and dealt with under guidance from HR.

Response to an Incident of Concern

Contacts

- Sheffield Safeguarding Advisory Desk 0114 205 3535
- e-Safety Project Manager
- Julia Codman 0114 293 6945
- Sheffield Police
  0114 220 2020
- Child Exploitation and Online Protection Centre (CEOP)
  www.ceop.police.uk