Meadowdale Academy E-Safety Policy

Mobile Device Usage

- The School strongly advises that student mobile devices should not be brought into school.
- The school accepts that a parent or carer may have good reason to request that their child carry a mobile device for use outside normal school hours.
- Student mobile phones which are brought into school must be turned off (not placed on silent) and stored in the appropriate box for the remainder of the day. Phones are collected in morning registration and are then returned at the end of the day. During this time they are locked in a secure place.
- Mobile devices brought into school and not handed in for safekeeping are entirely at the students own risk.
- If deemed necessary, the authorised member of staff can search the contents of a student's mobile device.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile device during the school day, but to contact the school office.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile devices will be released to parents or carers in accordance with the school policy.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.
- The recording, taking and sharing of images, video and audio on any mobile device is to be avoided; except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring.
- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time. They should be switched off or silent at all times. Unless requested by a member of staff.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.

Technical and Infrastructure approaches

This school:

- Has the educational filtered secure broadband connectivity through Northumberland County Council so connects to the 'private' National Education Network.
- Uses the Northumberland County Council filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy is logged and only available to staff with the approved 'web filtering management' status.
- Ensures network healthy through use of anti-virus software and network set-up so pupils cannot download executable files.
- Uses individual, audited log-ins for all pupils.
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform.
- Only unblocks other external social networking sites for specific purposes / Internet Literacy lessons.
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes at a regional or national level, such as Audio Network.
- Uses security time-outs on Internet access where practicable / useful.
- Works in partnership with the Northumberland County Council to ensure any concerns about the system are communicated so that systems remain robust and protect students.
- Ensures the Systems Administrator / network manager is up-to-date with Northumberland County Council services and policies / requires the Technical Support Provider to be up-to-date with Northumberland County Council services and policies.

Policy and procedures

This school:

- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access.
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns.
- Requires staff to preview websites before use.
- Informs users that Internet use is monitored.
- Informs staff and students that that they must report any failure of the filtering systems directly to the network technician.
- Requires pupils to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme.
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system.

- Ensures the named child protection officer has appropriate training.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc available for pupils, staff and parents.
- Provides Esafety advice for pupils, staff and parents.
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police – and the LA.

Education and training:

This school:

- Ensures pupils and staff know what to do if there is a cyber-bullying incident;
- Ensures all pupils know how to report any abuse;
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on national guidance. Pupils are taught a range of skills and behaviours appropriate to their age and experience, in accordance with the National Curriculum.
- Ensures that when copying materials from the web pupils understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights.
- Ensures that pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling.
- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection.

Digital Videos and Images

In this school:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school.
- Digital images /video of pupils are stored in a private teachers' shared images folder on the network and images are deleted at the end of their academy education – unless an item is specifically kept for a key school publication.
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs.
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils.
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose.
- Pupils are taught about how images can be manipulated in their eSafety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work.

- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identify of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

Website:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and the quality of presentation is maintained.
- Uploading of information is restricted to our website authorisers.
- The school web site complies with the school's guidelines for publications.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.
- The point of contact on the web site is the school address, telephone number and we use a general email contact address, admin@meadowdale.northumberland.sch.uk. Home information or individual e-mail identities will not be published.
- Photographs published on the web do not have full names attached.
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website.
- We expect teachers using' school approved blogs or wikis to password protect them and run from the school website.

Learning platform:

- Uploading of information on the schools' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas.
- Photographs and videos uploaded to the schools VLE will only be accessible by members of the school community.
- In school, pupils are only able to upload and publish within school approved and closed systems, such as the Learning Platform.
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' Learning Platform for such communications.

CCTV:

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings (retained by the Support Provider for 28 days), without permission except where disclosed to the Police as part of a criminal investigation.

Managing the Network and Equipment

To ensure the network is used safely this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password. We also use a different username and password for access to our school's network.
- Staff access to the schools' management information system is controlled through a separate password for data security purposes.
- We provide pupils with an individual network log-in username. From Year 5 they are also expected to use a personal password.
- All pupils have their own unique username and password which gives them access to the Internet.
- We make it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find.
- We make clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network.
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas.
- Requires all users to always log off when they have finished working or are leaving the computer unattended.
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day and we also automatically switch off all computers at 6 o'clock to save energy.
- Has set-up the network so that users cannot download executable files / programmes.
- Has blocked access to music download or shopping sites – except those approved for educational purposes.
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
  e.g. teachers access report writing module; SEN coordinator - SEN data.
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems.

- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data that complies with external Audit's requirements.
- All computer equipment is installed professionally and meets health and safety standards.
- Projectors are maintained so that the quality of presentation remains high.
- Reviews the school ICT systems regularly with regard to health and safety and security.
- Permits staff to only save in three places; a school provided encrypted memory stick, personal work area or Central Resources Staff. Any alternative locations must be discussed first with the authorised member of staff.

Staff use of personal devices

- Any permitted images or files taken in school must be downloaded from the device and deleted in school before the end of the day.
- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices will be switched off or switched to 'silent' mode. Bluetooth communication should be 'hidden' or switched off and mobile phones or personally-owned devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or a personally-owned device as part of an educational activity then it will only take place when approved by the senior leadership team.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.
- 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 students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

Roles & Responsibilities

Role	Key Responsibilities
Headteacher	• To take overall responsibility for E-Safety provision. • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring staff receive suitable training. • To be aware of procedures followed in the event of an incident
E-Safety Co-Ordinator/ Child protection Leader	• Takes day to day responsibility for E-Safety issues • Promotes an awareness of E-Safety procedures • Liaises with ICT Network staff • Communicates incidents back regularly to SLT • To ensure E-safety log is kept up to date • Is aware of any potential issues • To inform E-Safety governor of any issues
E- Safety Governor	• To ensure that the school follows correct E-Safety policies • To monitor the implementation of the E-Safety Policy in the school and to review its effectiveness. • To receive bi-annual reports on the feedback (in an agreed form) about the E-Safety Policy from the designated responsible members of staff.
Head of Computing	• To oversee the delivery of the E-Safety element of the computing curriculum. • To monitor the use of the school VLE • To monitor the use of ICT and the internet within Computing lessons and across the curriculum
Network Manager/Technician	• To report any E-Safety related issues that arise to the E-Safety Co-Ordinator • To ensure that users may only access the schools system via their own password and username • To ensure that provision exists for misuse detection and malicious attacks ie Viruses • To ensure the security of the ICT system • To ensure that access controls and encryption exist • To keep the schools policy on web filtering up to date

	• To keep up to date with E-Safety regulation and policy
Teaching staff	• To embed E-Safety issues within the curriculum • To supervise and guide pupils on the use of technology • To ensure that students are fully aware of research skills
All staff	• To read and understand the schools E-Safety policy • To read and accept the schools acceptable use policy • To be aware of issues from the use of mobile phones and how to deal with these (ie Turning off Bluetooth on their mobile phones) • To model safe and professional behaviours • To ensure that any digital communication with pupils is on a professional level and only through school based systems.
Pupils	• To read and understand the schools Acceptable policy and to have this signed by parents or carers • Have a good understanding of research skills • To use the school IT systems for school work and not personal use • To understand the importance of copyright and plagiarism • To know what action to take if an E-Safety incident occurs • To know the school policy on mobile phones and technical devices • To help the school in the creation of E-Safety policies.