



New Mills School

ONLINE SAFETY POLICY

Revision	Authorised by	Date	Adopted by	Date
Draft	K Lutener	April 2014		
Final	F&GP	July 2014	FGB Min No. 8	10/07/2014
Draft	Keith Lutener	July 2015	FGB Min No. 13	19/10/2015
Draft	Keith Lutener	May 2018		
Review	Garry Cash	November 2018	FGB Min No. 13i	26/02/2019

Revision	Date	Description of Changes
Draft	July 2015	Updated DCC Policy document
Draft	May 2018	Impero Safe guarding included (p5), e-Safety Coordinator updated
Review	November 2018	Updated Policy Template provided by DCC CPM (Schools)

Signed:M Cole..... Date:26/02/2019.....

Chair of Governors

Contents

	Page no
Key Details	4
Policy Aims	4
1. Policy Scope	5
1.2 Links with other policies and practices	5
2. Monitoring and Review	5
3. Roles and Responsibilities	6
3.1 The leadership and management team	6
3.2 The Designated Safeguarding Lead	6
3.3 Members of staff	7
3.4 Staff who manage the technical environment	7
3.5 Learners	8
3.6 Parents	8
4. Education and Engagement Approaches	8
4.1 Education and engagement with learners	8
4.2 Vulnerable Learners	9
4.3 Training and engagement with staff	9
4.4 Awareness and engagement with parents	10
5. Reducing Online Risks	10
6. Safer Use of Technology	11
6.1 Classroom Use	11
6.2 Managing Internet Access	11
6.3 Filtering and Monitoring	11
6.4 Managing Personal Data Online	12
6.5 Security and Management of Information Systems	12
6.6 Managing the Safety of the Website	13
6.7 Publishing Images and Videos Online	13
6.8 Managing Email	13
6.9 Educational use of Videoconferencing and/or Webcams	14
6.10 Management of Applications (apps) used to Record Learners Progress	15
7. Social Media	16
7.1 Expectations	16
7.2 Staff Personal Use of Social Media	17
7.3 Learners Personal Use of Social Media	18
7.4 Official Use of Social Media	18
8. Use of Personal Devices and Mobile Phones	20
8.1 Expectations	20
8.2 Staff Use of Personal Devices and Mobile Phones	20
8.3 Learners Use of Personal Devices and Mobile Phones	21
8.4 Visitors' Use of Personal Devices and Mobile Phones	22
8.5 Officially provided mobile phones and devices	22
9. Responding to Online Safety Incidents and Concerns	22
9.1 Concerns about Learner Welfare	22

9.2 Staff Misuse	23
10. Procedures for Responding to Specific Online Incidents or Concerns	23
10.1 Online Sexual Violence and Sexual Harassment between Children	23
10.2 Youth Produced Sexual Imagery or “Sexting”	24
10.3 Online Child Sexual Abuse and Exploitation	25
10.3 Indecent Images of Children (IIOC)	26
10.5 Cyberbullying	27
10.6 Online Hate	27
10.7 Online Radicalisation and Extremism	27
11. Useful Links for Educational Schools	28

New Mills School Online Safety Policy

Key Details

Designated Safeguarding Lead (DSL): Ian Withers (Assistant Headteacher)
Debbie McGloin (Headteacher)

Named Governor with lead responsibility: Maggie Cole (Chair of Governors)

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure

Policy Aims

- This online safety policy has been written by New Mills School, building on the Kent County Council/The Education People online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance '[Keeping Children Safe in Education](#)' 2018, '[Working Together to Safeguard Children](#)' 2018 and the [Derbyshire Safeguarding Children Board](#) procedures.
- The purpose of New Mills School Online Safety Policy is to:
 - Safeguard and protect all members of community online.
 - Identify approaches to educate and raise awareness of online safety throughout the community.
 - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology.
 - Identify clear procedures to use when responding to online safety concerns.
- New Mills School identifies that the issues classified within online safety are considerable, but can be broadly categorised into three areas of risk:
 - **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.

1. Policy Scope

- New Mills School believes that online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- New Mills School identifies that the internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- New Mills School believes that learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as “staff” in this policy) as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

1.1 Links with other policies and practices

This policy links with several other policies, practices and action plans including:

- Anti-bullying policy
- Acceptable Use Policies (AUP) and/or the Code of conduct/staff behaviour policy
- Behaviour and discipline policy
- Child protection policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data security
- Image use policy
- Mobile phone and social media policies
- Searching, screening and confiscation policy

2. Monitoring and Review

- Technology in this area evolves and changes rapidly. New Mills School will review this policy at least annually.
 - The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the Headteacher will be informed of online safety concerns, as appropriate.

- The named governor for safeguarding will report on a regular basis to the governing body on online safety practice and incidents, including outcomes.
- Any issues identified via monitoring will be incorporated into our action planning.

3. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL) Ian Withers, Assistant Headteacher, has lead responsibility for online safety. Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL.
- New Mills School recognises that all members of the community have important roles and responsibilities to play with regards to online safety.

3.1 The leadership and management team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety; including a staff code of conduct/behaviour policy and acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

3.2 The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- Work alongside deputy DSLs to ensure online safety is recognised as part of the schools safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant knowledge and up to date required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.

- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the schools safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the school management team and Governing Body.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding *and/or* online safety.

3.3 It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of school systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the schools safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.

3.4 It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the DSL and leadership team to ensure that the schools IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.
- Ensure that our filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team

- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

3.5 It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

3.6 It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home-school agreement and acceptable use policies.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

4. Education and Engagement Approaches

4.1 Education and engagement with learners

- The school will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
 - Ensuring education regarding safe and responsible use precedes internet access.
 - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
 - Reinforcing online safety messages whenever technology or the internet is in use.
 - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
 - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

- The school will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
 - Displaying acceptable use posters in all rooms with internet access.
 - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
 - Rewarding positive use of technology.
 - Implementing appropriate peer education approaches.
 - Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
 - Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
 - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

4.2 Vulnerable Learners

- New Mills School recognises that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- New Mills School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners.
- When implementing an appropriate online safety policy and curriculum New Mills School will seek input from specialist staff as appropriate, including the SENCO, Child in Care Designated Teacher.

4.3 Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
 - This will cover the potential risks posed to learners (Content, Contact and Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the school, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.

- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

4.4 Awareness and engagement with parents and carers

- New Mills School recognises that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:
 - Providing information and guidance on online safety in a variety of formats.
 - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
 - Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
 - Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
 - Requiring them to read our acceptable use policies and discuss the implications with their children.

5. Reducing Online Risks

- New Mills School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
 - Regularly review the methods used to identify, assess and minimise online risks.
 - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the school is permitted.
 - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
 - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

6. Safer Use of Technology

6.1 Classroom Use

- New Mills School uses a wide range of technology. This includes access to
 - Computers, laptops and other digital devices
 - Internet which may include search engines and educational websites
 - Impero Classroom Management for monitoring and filtering services
 - Learning platform/intranet
 - Email
 - Digital cameras, web cams and video cameras
- All school owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- The school will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and learners complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
 - **Key Stage 3 and 4**
 - Learners will be appropriately supervised when using technology, according to their ability and understanding.

6.2 Managing Internet Access

- We will maintain a written record of users who are granted access to our devices and systems.
- All staff, learners and visitors will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

6.3 Filtering and Monitoring

6.3.1 Decision Making

- New Mills School governors and leaders have ensured that our school has age and ability appropriate filtering and monitoring in place, to limit learner's exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

6.3.2 Filtering

- Education broadband connectivity is provided through KCom.
- We use (Netsweeper & Impero Classroom Management) filtering sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- The filtering system blocks all sites on the [Internet Watch Foundation](#) (IWF) list.
- We work with (Impero//Netsweeper) to ensure that our filtering policy is continually reviewed.
- If learners discover unsuitable sites, they will be required to:
 - turn off monitor/screen and report the concern immediate to a member of staff.
 - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
 - The breach will be recorded and escalated as appropriate.
 - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF or CEOP.

6.3.3 Monitoring

- We will appropriately monitor internet use on all school owned or provided internet enabled devices. This is achieved by:
 - Users are monitored through the use of Impero Classroom Management software, which fully logs and alerts to breaches of internet rules. Logs are viewed on request by staff with full tracking available for web usage when required. Teachers and IT staff monitor lessons through the use of the software, making necessary changes where required. Any breaches are logged and screen shots immediately taken for later perusal as needed.
- Concerns blocked via monitoring are checked and passed to Year Managers who will then contact the DSL depending on severity or pass to relevant member of SLT. Who will in return respond by following the New Mills School Child Protection Policy? All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

6.4 Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection Policies and legislation.

6.5 Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
 - Virus protection being updated regularly.

- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
- Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
- Not downloading unapproved software to work devices or opening unfamiliar email attachments.
- Regularly checking files held on our network,
- The appropriate use of user logins and passwords to access our network.
 - Specific user logins and passwords will be enforced for all users
- All users are expected to log off or lock their screens/devices if systems are unattended.

6.5.1 Password policy

All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

- All learners are provided with their own unique username and private passwords to access our systems; learners are responsible for keeping their password private.
- We require all users to:
 - Use strong passwords for access into our system.
 - Change their passwords every 90 days.
 - Always keep their password private; users must not share it with others or leave it where others can find it.
 - Not to login as another user at any time.

6.6 Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learner's personal information will not be published on our website; the contact details on the website will be our school address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

6.7 Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated policies, including (but not limited to) the: cameras and image use, data security, GDPR, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

6.8 Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.
 - The forwarding of any chain messages/emails is not permitted.
 - Spam or junk mail will be blocked and reported to the email provider.
 - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
 - School email addresses and other official contact details will not be used for personal social media accounts.
- Members of the community should immediately tell (*name and role of designated member of staff*) if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.
- We will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff.

6.8.1 Staff email

- The use of personal email addresses by staff for any official school business is not permitted.
 - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

6.8.2 Learner email

- Learners will use provided email accounts for educational purposes.
- Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

6.9 Educational use of Videoconferencing

- New Mills School recognise that videoconferencing can be a challenging activity but brings a wide range of learning benefits.
 - All videoconferencing equipment will be switched off when not in use and will not be set to auto-answer.
 - Video conferencing equipment connected to the educational broadband network will use the national E.163 numbering system and display their H.323 ID name; external IP addresses will not be made available to other sites.
 - Videoconferencing contact details will not be posted publically.
 - Videoconferencing equipment will not be taken off the premises without prior permission from the DSL.

- Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
- Video conferencing equipment will be kept securely and, if necessary, locked away or disabled when not in use.

6.9.1 Users

- Parents/carers consent will be obtained prior to learners taking part in videoconferencing activities.
- Learners will ask permission from a member of staff before making or answering a videoconference call or message.
- Videoconferencing will be supervised appropriately, according to the learners age and ability.
- Video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages.
- The unique log on and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

6.9.2 Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and written permission will be obtained from all participants; the reason for the recording must be given and recorded material will be stored securely.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

6.10 Management of Applications (apps) used to Record Children's Progress (*If used*)

- We use (*insert name of system*) to track learners progress and share appropriate information with parents and carers.
- The *Headteacher* (*amend as appropriate*) is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learner's data:
 - Only learner issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
 - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.

- Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
- All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

7. Social Media

7.1 Expectations

- The expectations' regarding safe and responsible use of social media applies to all members of New Mills School community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of New Mills School community are expected to engage in social media in a positive, safe and responsible manner.
 - All members of New Mills School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Neither staff nor pupils are permitted to access social media in school time
 - Any use of social media during school hours or whilst using school devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of New Mills School community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

7.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.
 - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
 - School the privacy levels of their personal sites.
 - Being aware of location sharing services.
 - Opting out of public listings on social networking sites.
 - Logging out of accounts after use.
 - Keeping passwords safe and confidential.
 - Ensuring staff do not represent their personal views as that of the school.
- Members of staff are encouraged not to identify themselves as employees of New Mills School on their personal social networking accounts; this is to prevent information on these sites from being linked with the school, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
 - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputy) and/or the Headteacher.
 - If ongoing contact with learners is required once they have left the school, members of staff will be expected to use existing alumni networks or use official school provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the Headteacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

7.3 Learners Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore we will not create accounts specifically for learners under this age.
- Any concerns regarding learners use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.

- Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
 - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
 - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
 - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
 - To use safe passwords.
 - To use social media sites which are appropriate for their age and abilities.
 - How to block and report unwanted communications.
 - How to report concerns both within the school and externally.

7.4 Official Use of Social Media

New Mills School official social media channels are:

- <https://www.facebook.com/newmillsschool>
- <https://twitter.com/NewMillsSchool>
- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
 - The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher.
 - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
 - Staff use school provided email addresses to register for and manage any official social media channels.
 - Official social media sites are suitably protected and, where possible, run and linked to/from our website.
 - Public communications on behalf of the school will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection.
 - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
 - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
 - Any official social media activity involving learners will be moderated.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.

- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the school, they will:
 - Sign our social media acceptable use policy.
 - Always be professional and aware they are an ambassador for the school.
 - Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the school.
 - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
 - Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
 - Ensure that they have appropriate consent before sharing images on the official social media channel.
 - Not disclose information, make commitments or engage in activities on behalf of the school, unless they are authorised to do so.
 - Not engage with any direct or private messaging with current, or past, learners, parents and carers.
 - Inform their line manager, the DSL (or deputy) and/or the Headteacher of any concerns, such as criticism, inappropriate content or contact from learners.

8. Use of Personal Devices and Mobile Phones

- New Mills School recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the school.

8.1 Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and ‘smart’ watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
 - All members of New Mills School community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
 - All members of New Mills School community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms and toilets.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of New Mills School community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.

8.2 Staff Use of Personal Devices and Mobile Phones

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as, relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
- Staff will be advised to:
 - Keep mobile phones and personal devices in a safe and secure place during lesson time.
 - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
 - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
 - Not use personal devices during teaching periods, unless written permission has been given by the Headteacher, such as in emergency circumstances.
 - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are not permitted to use their own personal phones or devices for contacting learners or parents and carers.
 - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy) and/or Headteacher.
- Staff will not use personal devices:
 - To take photos or videos of learners and will only use work-provided equipment for this purpose.
 - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
 - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the police will be contacted.

8.3 Learners Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- New Mills School expects learners' personal devices and mobile phones which are brought into school to be turned off (not placed on silent) and stored out of sight immediately the

student arrives at the school gate. They must remain turned off and out of sight until the student has left the school site at the end of their day. This includes break time and lunch time.

- If a learner needs to contact his/her parents or carers they will be allowed to use a school phone, located close to the Head's PA office
 - Parents are advised to contact their child via the school office
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time
 - If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- Mobile phones and personal devices must not be taken into examinations.
 - Learners found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
 - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
 - Mobile phones and devices that have been confiscated will be released in accordance with the school's Mobile Phone Policy

8.4 Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Headteacher of any breaches our policy.

8.5 Officially provided mobile phones and devices

- School mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.
- The school currently has two mobile phones
 - For caretaker use
 - For use on school trips

9. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
 - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- If we are unsure how to proceed with an incident or concern, the DSL (or deputy) will seek advice.

9.1 Concerns about Learners Welfare

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
 - The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Derbyshire Safeguarding Children's Board (DSCB) thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

9.2 Staff Misuse

- Any complaint about staff misuse will be referred to the Headteacher, in accordance with the allegations policy.
- Any allegations regarding a member of staff's online conduct will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

10. Procedures for Responding to Specific Online Incidents or Concerns

10.1 Online Sexual Violence and Sexual Harassment between Children

- Our school has accessed and understood "[Sexual violence and sexual harassment between children in schools and colleges](#)" (2018) guidance and part 5 of 'Keeping children safe in education' 2018.
- New Mills School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
 - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- New Mills School recognises that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- New Mills School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- New Mills School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
 - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
 - If content is contained on learners electronic devices, they will be managed in accordance with the DfE '[searching screening and confiscation](#)' advice.

- Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies.
- If the concern involves children and young people at a different educational school, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
 - If a criminal offence has been committed, the DSL (or deputy) will discuss this with local Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

10.2 Youth Produced Sexual Imagery (“Sexting”)

- New Mills School recognises youth produced sexual imagery (known as “sexting”) as a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy).
- We will follow the advice as set out in the non-statutory UKCCIS guidance: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) and [KSCB guidance: “Responding to youth produced sexual imagery”](#).
- New Mills School will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of ‘sexting’ by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- We will ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- We will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using school provided or personal equipment.
- We will not:
 - View any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so.
 - If it is deemed necessary, the image will only be viewed by the DSL (or deputy DSL) and their justification for viewing the image will be clearly documented.
 - Send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request learners to do so.
- If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:
 - Act in accordance with our child protection policies and the relevant DSCB’s procedures.
 - Ensure the DSL (or deputy) responds in line with the [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) guidance.
 - Store the device securely.
 - If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image.

- Carry out a risk assessment which considers any vulnerability of learners involved; including carrying out relevant checks with other agencies.
- Inform parents and carers, if appropriate, about the incident and how it is being managed.
- Make a referral as deemed appropriate in line with the UKCCIS : [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) guidance.
- Provide the necessary safeguards and support for learners, such as offering counselling or pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy but taking care not to further traumatise victims where possible.
- Consider the deletion of images in accordance with the UKCCIS: [‘Sexting in schools and colleges: responding to incidents and safeguarding young people’](#) guidance.
 - Images will only be deleted once the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- Review the handling of any incidents to ensure that best practice was implemented; the leadership team will also review and update any management procedures, where necessary.

10.3 Online Child Sexual Abuse and Exploitation (including child criminal exploitation)

- New Mills School will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- New Mills School recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the ‘Click CEOP’ report button is visible and available to learners and other members of our community. (*Include where this can be accessed, e.g. website, intranet, etc.*)
- If made aware of incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:
 - Act in accordance with our child protection policies and the relevant DSCB’s procedures.
 - If appropriate, store any devices involved securely.
 - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
 - Inform parents/carers about the incident and how it is being managed.

- Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
- Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using school provided or personal equipment.
 - Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/
- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Safeguarding Team and/or the Police.
- If made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the [Child Sexual Exploitation Team](#) (CSET) by the DSL (or deputy).
- If learners at other school are believed to have been targeted, the DSL (or deputy) will seek support to ensure that potential investigations are not compromised.

10.4 Indecent Images of Children (IIOC)

- New Mills School will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through DSCB.
- If made aware of IIOC, we will:
 - Act in accordance with our child protection policy and the relevant DSCB procedures.
 - Store any devices involved securely.
 - Immediately inform appropriate organisations
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
 - Ensure that the DSL (or deputy) is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
 - Ensure that any copies that exist of the image, for example in emails, are deleted.
 - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the school provided devices, we will:
 - Ensure that the DSL (or deputy) is informed.
 - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .

- Ensure that any copies that exist of the image, for example in emails, are deleted.
- Inform the police via 101 (999 if there is an immediate risk of harm) and Children’s Social Work Service (as appropriate).
- Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:
 - Ensure that the Headteacher is informed in line with our managing allegations against staff policy.
 - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
 - Quarantine any devices until police advice has been sought.

10.5 Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at New Mills School.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

10.6 Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at New Mills School and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through the Education Safeguarding Team and/or the Police.

10.7 Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.
- If we are concerned that a child or parent/carers may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the Headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

12. Useful Links for Educational Schools

DSCB:

- <https://www.derbyshirescb.org.uk/home.aspx>

National Links and Resources for Educational Schools

- CEOP:
 - www.thinkuknow.co.uk
 - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
 - Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk

National Links and Resources for Parents/Carers

- Action Fraud: www.actionfraud.police.uk
- CEOP:
 - www.thinkuknow.co.uk
 - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
 - ChildLine: www.childline.org.uk
 - Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

Acknowledgement

Please note that the copyright of this document and materials is held by The Education People.

Disclaimer

The Education People make every effort to ensure that the information in this document is accurate and up-to-date. If errors are brought to our attention, we will correct them as soon as practicable.

The copyright of these materials is held by The Education People. However, educational schools that work with children and young people are granted permission to use all or part of the materials for not for profit use, providing the Education People copyright is acknowledged and we are informed of its use.