LET RIGHT BE DONE

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
Review	Emma Adrio	February 2024	FGB Min No. 16	28/03/2024

Revision	Date	Description of Changes
Draft	July 2015	Updated DCC Policy document
Draft	May 2018	Impero Safeguarding included (p5) e-safety coordinator updated
Review	November 2018	Updated Policy Template provided by DCC CPM (Schools)
Review	February 2024	Updated Policy Template Review by E Adrio

Signed: ……………..………………… Date: ………………….……….
Chair of Governors

Policy purpose and summary

This Policy outlines the schools' approach to ensuring that everyone can work safely online. It sets out individual responsibilities to ensure compliance with this Policy.

Related policies or guidance:

- Data Protection Policy for Staff
- IT Acceptable Use Policy
- Social Media Policy
- Acceptable Use of Mobile Phones Policy
- Ready to Learn Behaviour Policy
- Child Protection & Safeguarding Policy

Online Safety Policy

1. Introduction and Purpose

1.1. New Mills School is committed to promoting the welfare and safety of our students when using digital and online technologies. New Mills School recognises the importance of the contribution it can make to protecting and supporting students in their use of these technologies.

1.2. This policy is designed to incorporate all aspects of child protection and safeguarding that may be affected by digital technology, mobile phone technology, as well as use of technology within school.

1.3. New Mills School will refer to the most recent government, Department for Education (DfE) and Information Commissioners Office (ICO) guidance and documentation with regard to data protection, data storage and privacy compliance.

2. Scope

2.1. This policy applies to all New Mills School staff (including agency), pupils/students, parents/carers, Governors, and other volunteers.

2.2. This policy applies to any individual who is given access to New Mills School's digitally connected systems (including email addresses and any other data source or system that is hosted/operated/controlled remotely or other by the organisation).

2.3. New Mills School will make use of relevant legislation and guidelines to affect positive behaviour regarding the use of technology and the Internet both on and off the school site. This will include imposing rewards and sanctions for behaviour - as defined as regulation or student behaviour under the Education and Inspections Act 20065 . The 'In Loco Parentis' duty allows the school to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

2.4. As identified by Keeping Children Safe in Education, this policy recognises that technology plays a significant role in children's lives and abuse can take place concurrently online and in daily life. Online safety must therefore be considered as part of a whole school approach.

2.5. The Online Safety Policy covers the use of:

▪ School based IT systems and cloud-based software;

▪ School based intranet and networking;

▪ School related external Internet, including but not exclusively, extranet, e-learning platforms, blogs, social media websites;

▪ External access to internal school networking, such as webmail, network access, fileserving (document folders) and printing;

▪ School IT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets, dongles;

▪ Student and staff personal IT equipment when used in school and which makes use of school networking, file-serving, or Internet facilities;

▪ Tablets, mobile phones, devices, and laptops when used on the school site.

3. Policy Statement

3.1. The definition of an online incident is:

"Any incident that occurs and involves any person (student or adult) where the use of technology (equipment and/or networks) enables or facilitates inappropriate behaviour and harm and/or distress is caused to another person or the reputation of the school. This may include the use of social media, forums, blogs, open and closed groups, digital images, messages, or any other means."

3.2. The most likely areas of risk to students are:

▪ Exposure to illegal inappropriate or harmful material;

▪ Subject to harmful online interactions with other users;

▪ The individual's personal online risky behaviour that then leads to harm.

▪ Online 'commerce' (online gambling, inappropriate advertising, phishing, or financial scams)

3.3. New Mills School has a responsibility for ensuring that the resources are available to promote the safe use of technology and to promote understanding and awareness of the risks attached to the use of digital technology.

3.4. We seek to promote the use of technology and connectivity to ensure that the students are equipped with the necessary skills and knowledge to perform to the best of their ability both during their time in school and in their future in their chosen careers and workplaces.

3.5. Staff and students must be able to use digital technology appropriately and safely and understand the risks related to their activity. Students will receive online safety education as soon as they start using digital technology and this will be continually reinforced and monitored as students' progress through their school life.

3.6. New Mills School actively encourages a proactive approach to new and emerging technologies and threats to mitigate the risk of harm to students, staff and the trust and associated academies and their reputations. We seek to promote a 'cyber aware' culture that ensures all staff, students and trustees take part in and continue to develop their knowledge and understanding of online behaviour and in particular, how to prevent harm through continual learning resources, research, and encouragement from all teachers.

4. Standards and Expectations

4.1. Systems

4.1.1. New Mills School's computer systems will be configured to ensure the teaching and learning requirements of the school are met whilst ensuring online safety is maintained.

4.1.2. Risk assessments are completed (a Data Privacy Impact Assessment, DPIA) when there is a major overhaul to the system or a new cloud-based software package is purchased, for example.

4.1.3. The system will be compliant with the school, local authority, DfE, ICO and Data Protection guidelines with regard to online safety procedures being met.

4.1.4. Regular audits and evaluations of the IT network will be carried out, identifying where improvements can be made.

4.1.5. New Mills School IT staff will be responsible for monitoring IT use.

4.2. Filtering & Monitoring

4.2.1. The school will ensure an accredited filtering system is used. Filtering reports and logs will be examined regularly.

4.2.2. The school will ensure an accredited monitoring system is used. Monitoring reports and logs will be examined regularly.

4.2.3. Any filtering incidents are examined, and action taken and recorded to prevent a recurrence. The school will provide enhanced/differentiated user-level filtering. Internet access will be filtered for all users.

4.3. Network security

4.3.1. All users will have clearly defined access rights to school technical systems and devices.

4.3.2. All users will be provided with a username and secure password by New Mills School IT staff. Users are responsible for the security of their username and password.

4.3.3. The Network Manager and Headteacher/other designated senior person will have access to the main administrator password.

4.3.4. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations etc. from accidental or malicious attempts which might threaten the security of the academy systems and data.

4.4. Use of images and videos

4.4.1. The school will ensure images and videos of students, staff, students' work and any other personally identifying material are used, stored, archived, and published in line with the Data Protection Act, ICO guidance for schools, DfE guidance for schools and the Acceptable Use Policy.

4.4.2. When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images, in particular the risks attached to publishing their own images on the Internet e.g., social media sites.

4.4.3. Written permission from parents/carers will be obtained before photographs of students are published on the school website/social media/local press.

4.4.4. In accordance with guidance from the ICO, parents can take videos and digital images of their children at school events for their own personal use but should not be made publicly available where other students are involved in the digital image or video.

4.4.5. Students must not take, use, share, publish or distribute images of others without their permission.

4.5. Data Protection

4.5.1. Personal data will be recorded, processed, transferred, and made available according to the school's Data Protection Policy and in compliance with GDPR and the Data Protection Act (1998).

4.6. Social Media

4.6.1. Staff, governors, students and volunteers are expected to comply with the Trust's Social Media Policy.

5. Responsibilities

5.1. The Headteacher will ensure that all staff and visitors are aware of the Online Safety Policy and procedure and of their responsibilities set out in this policy. It is the responsibility of the Headteacher to ensure that breaches of the policy are investigated and addressed.

5.2. Staff, governors, students and volunteers are expected to adhere to the policy and procedure and ensure that they conduct themselves in a manner that will not place students or vulnerable adults at risk, bring the school into disrepute or damage their own professional reputation.

5.3. School management and online safety

5.3.1. The Senior Leadership Teams (SLTs) are responsible for determining, evaluating and reviewing online safety to encompass teaching and learning, use of scholl IT equipment and facilities by students, staff and visitors, and agreed criteria for acceptable use by students, school staff of Internet capable equipment for school related purposes, or in situations which will impact on the reputation of the school, and/or on school premises. This is in line with expectations in Keeping Children Safe in Education in relation to an annual review/risk assessment of online safety provision.

5.3.2. Regular assessment of the strengths and weaknesses of practice within the school will help determine INSET provision needed for staff and guidance provided to parents, students, and local partnerships.

5.4. Online Safety Co-ordinator

5.4.1. The school has a designated Online Safety Co-ordinator who reports to the Senior Leadership Team and coordinates online safety provision across the school community.

5.4.2. The school's Online Safety Co-ordinator is responsible for online safety issues on a day-to-day basis and also liaises with relevant stakeholders including IT support to ensure the safety of students.

5.4.3. The Online Safety Co-ordinator maintains a log of submitted online safety reports and incidents.

5.4.4. The Online Safety Co-ordinator audits and assesses inset requirements for staff, support staff online safety training, and ensures that all staff are aware of their responsibilities and the school's online safety procedures. The Co-ordinator is also the first port of call for staff requiring advice on online safety matters.

5.4.5. The Online Safety Co-ordinator is responsible for promoting best practice in online safety within the wider school community, including providing and being a source of information for parents and partner stakeholders. This may include facilitating regular assemblies and other such activities that focus on positive messages and behaviours.

5.4.6. The Online Safety Co-ordinator will be involved in any risk assessment of new technologies, services, or software to analyse any potential risks.

5.5. IT support staff

5.6.1. Internal IT support staff are responsible for maintaining the school's networking, IT infrastructure and hardware. IT staff will be aware of current thinking and trends in IT security and ensure that the school system, particularly file-sharing and access to the Internet, is secure. IT staff will ensure systems are not open to abuse or unauthorised external access.

5.6.2. IT support staff in school is responsible for:

▪ Defending the network and infrastructure of the school, reviewing activity logs regularly;

▪ Ensuring that users comply with basic access policies and that only trusted devices can connect to the school network;

▪ Filtering of search facilities is robust and regularly checked for penetration to ensure that the risk of students accessing material that is unsuitable is minimised;

▪ To keep up to date with current threats and attack trends and take steps to mitigate this and communicate with the management team and Online Safety Co-ordinator;

▪ To report to the management team and Online Safety Co-ordinator on any network intrusions or other threats to the network;

▪ To ensure that any IT outsourced e.g., connectivity, maintenance, cloud based services website, email provision, filtering, anti-virus, complies with DfE guidance and Data Protection regulations;

▪ Promoting basic cyber security practices within the school e.g., locking computers when away from the desk, using secure passwords, caution when using USB removable drives.

5.6.3. External contractors, website designers/hosts will be made fully aware of and agree to the School's Online Safety Policy.

5.7. All Staff

5.7.1. Teaching and support staff are responsible for ensuring that they understand the school's Online Safety Policy, practices, and associated procedures for reporting online safety incidents in line with school procedures.

5.7.2. All staff will be provided with an online safety induction as part of the overall staff induction procedures. All staff will attend mandatory online safety training provided by the school.

5.7.3. All staff will ensure that they have read, understood, and signed the Acceptable Use Policy relevant to Internet and computer use in each academy.

5.7.4. All teaching staff are to be vigilant in monitoring student Internet and computer usage in line with the policy. This may include the use of personal technology, such as cameras and phones on the school site where there is a cause for concern.

5.7.5. Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

5.7.6. Staff must promote and reinforce safe online practices when on and off-site, including providing advice to students on how to report incidents.

5.7.7. Staff must report as soon as is practicable any suspected misuse of school's digitally connected systems to the Headteacher or Online Safety Co-ordinator.

5.8. Designated Safeguarding Lead (DSL)

5.8.1. The DSL will be trained in specific online safety issues e.g., CEOP accredited course or equivalent.

5.8.2. The DSL will be responsible for escalating online safety incidents to the relevant external parties e.g., CEOP, Cyber Choices, National Cyber Security Centre, local Police, Local Safeguarding Children's Board, social care and parents. Possible scenarios might include:

▪ Allegations against members of staff;

▪ Cybercrime – illegal hacking, denial of service, use of malware;

▪ Allegations or evidence of 'grooming;'

▪ Allegations or evidence of cyber bullying in the form of threats of violence, harassment, or a malicious communication;

▪ Sharing of indecent images including nudes or semi-nudes (consensual or non-consensual)

▪ Sexual violence or harassment between peers (child on child abuse).

5.8.3. The DSL is responsible for acting 'in loco parentis' and liaising with websites and social media platforms, such as Twitter and Facebook, to remove instances of illegal material or cyber bullying.

5.9. Pupils/Students

5.9.1. Pupils/students must ensure use of school Internet and computer systems in agreement with the terms specified in the policy

5.9.2. Students are responsible for ensuring they report online safety incidents in the school or with other external reporting facilities, such as CEOP or Childline, and are expected:

- To be aware of and comply with school policies for Internet and mobile technology usage in the school, including the use of personal items such as mobile phones;
- To be aware that their Internet use out of the school on social networking sites, is covered under the Online Safety Policy if it impacts on the school and/or its staff and students in terms of cyber bullying, reputation, or illegal activities;
- To follow basic cyber security practices within the school e.g., locking computers when away from the desk, using secure passwords, caution with use of USB removable drives.

5.10. Parents/Carers

5.10.1. Parents/carers must support the school in its promotion of good Internet behaviour and responsible use of IT equipment and mobile technologies both at school and at home.

5.10.2. Where appropriate, parents should sign the school's Acceptable Use Policy, indicating agreement regarding their child's user and also their own use with regard to parental access to school systems such as websites, forums, social media, online reporting arrangements and questionnaires.

5.11 Remote Education

5.11.1. Schools will have due regard to the DfE's 'Providing remote education: guidance for schools' after the expiration of the temporary provisions in the Coronavirus Act

6 Review

6.10 This policy will be monitored as part of the school's annual internal review and reviewed on a two-year cycle or as required by legislation changes.

6.11 An up-to-date copy of the policy will be available on the school website.