Moorside High School
Enriching Lives, Inspiring Ambitions

Online Safety and Mobile Technology

Policy

2021/2022

Date of Approval:	
Approved by:	Local Academy Board
Date of next Review:	

Contents

Scope of the Policy 3
Roles and Responsibilities 3
Online Safety Education and Training 5
Communication Devices And Methods 5
Good Practice Guidelines 6
Sexting / Peer on Peer Abuse / Cyberbullying 8
Searching Devices, Viewing And Deleting Imagery 8
Filtering and Monitoring 8
Information And Support 9
Complaints 9

Scope of the Policy

This policy applies to all members of the school community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of school.

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the school:

Academy Board Members:

- Academy Board Members (ABMs) are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including Online Safety) of members of the school community
- The Headteacher and at least one other member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff

Online safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The Headteacher ensures that the policy is implemented and compliance with the policy monitored. The responsibility for Online Safety has been designated to a member of the senior management team.

Online Safety Coordinator:

Our school Online Safety Coordinator is Mr P Livesey. The Online Safety Coordinator:

- Takes day to day responsibility for Online Safety issues and has a lead role in establishing and reviewing the school Online Safety policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place
- Provides training and advice for staff
- Receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments
- Reports regularly to the Senior Leadership Team

On Site Technician:

The onsite RM technician is responsible for ensuring:

- that the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- that the school meets the Online Safety technical requirements outlined in any relevant Local Authority Online Safety Policy and guidance
- that users may only access the school's networks through a properly enforced password protection policy

Teaching and Support Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following schoolOnline

Safety procedures. Central to this is fostering a 'no blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

Teaching and support staff are also responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current school Online Safety policyand practices
- they have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- they report any suspected misuse or problem to the Online Safety Co-ordinator or senior leader for investigation, action and possible sanction

All staff should be familiar with the school's policy including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of pupil information/photographs and use of website
- Online bullying procedures
- Their role in providing Online Safety/acceptable ICT use education for pupils
- Their role in preventing terrorism and extremism

Staff are reminded / updated about Online Safety matters at least once a year.

Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) should be trained in Online Safety issues and be aware of the potential forserious child Protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils

- are responsible for using the school ICT systems and mobile technologies in accordance with the Pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- must understand the importance of reporting abuse, misuse or access to inappropriate materials and knowhow to do so

We include Online Safety in the curriculum and ensure that every pupil has been educated about safe and responsible use. Pupils need to know how to minimise online risks and how to report a problem.

Parents/Carers

The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local Online Safety campaigns and literature. Parentsand carers will be responsible for:

- endorsing (by signature) the Student/Pupil Acceptable Use Policy
- accessing the school ICT systems or Learning Platform in accordance with the school Acceptable Use Policy

Online Safety Education and Training

Education – Pupils

Online Safety education will be provided in the following ways

- A planned Online Safety programme will be provided as part of ICT lessons and will be regularly revisited -this will cover both the use of ICT and new technologies both in and outside of school
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies
- Pupils will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

Education & Training – Staff

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff will receive Online Safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy and Acceptable Use Policies

Communication Devices And Methods

Pupils

Mobile phones are not permitted during the school day. Under exceptional circumstances, as directed by a member of staff, pupils may be permitted to take photographs of work. They may also be used for retrieving email.

Staff

Staff are permitted to have a mobile phone on their person and may use this for email, agreed school messenger services and for taking photographs for **school use only**.

Unsuitable / Inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school contextand that users, as defined below, should not engage in these activities in school or outside school when using schoolequipment or systems. The school policy restricts certain internet usage as follows:

- child sexual abuse images
- promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- extremist or terrorism related material
- pornography
- promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, ageand disability
- promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- using school systems to run a private business
- using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards

employed by SCC and / or the school

- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- on-line gaming (educational)
- on-line gaming (non educational)
- on-line gambling
- accessing the internet for personal or social use (e.g. online shopping, banking etc)
- file sharing e.g. music, films etc
- use of social networking sites
- use of video broadcasting eg Youtube, unless for educational purposes
- using external data storage devices (e.g. USB) that have not been encrypted (password protected and checked for viruses)

Good Practice Guidelines

Email		
Best Practice	**Safe Practice**	**Poor Practice**
Staff and pupils should only use their school email account to communicate with each other.	Check the school e-safety policy regarding the use of your school email or internet for personal use.	Staff should not use their personal email account to communicate with pupils and their families without a manager's knowledge or permission and in accordance with the school's e-safety policy.
Images, Photos &Videos		
Best Practice	**Safe Practice**	**Poor Practice**
Only use school equipment for taking pictures and videos. Ensureparental permission is in place.	Check the e-safety policy for any instances where using personal devices may be allowed. Always make sure you have the Head teacher / Senior Leader's	Do not download images from school's equipment to your own. Do not use your own equipment without the permission of the Headteacher / Senior Leader and in
	permission. Make arrangements for pictures to be downloaded to the school network immediately after an event.Delete images from the device after downloading.	accordance with the e-safety policy.Do not retain, copy or distribute images for your personal use.
Internet		

Best Practice	Safe Practice	Poor Practice
Understand how to search safely online and how to report inappropriate content.	Staff and pupils should be aware that monitoring software will log online activity. Be aware that keystroke monitoring software does just that. This means that if you are online shopping, then your passwords, credit card numbers and security codes will all be visible to the colleagues monitoring activity.	Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings. Beach of the e-safety and acceptable use policies may result inconfiscation of equipment, closing of accounts and instigation of sanctions.
Mobile Phones		
Best Practice	**Safe Practice**	**Poor Practice**
If on school business, school will provide appropriate equipment. Ensure you are aware of inbuilt software / facilities and switch it offif appropriate.	Check the e-safety policy for any instances where using personal phones may be allowed. Staff should be aware of how to conceal your number.	Do not use your own phone withoutthe permission of the Head teacher / Senior Leader. Do not retain pupil / parental detailsfor your own personal use.
Social Networking		
Schools should take into consideration the age of their pupils, and whether they are old enough to have accounts when including this guidance.		
Best Practice	**Safe Practice**	**Poor Practice**
If you have a personal account, regularly check all settings and make sure your security settings are not open access.	Do not accept people you do not know as friends. Be aware that belonging to a 'group' can allow access to your profile.	Do not have an open access profile that includes inappropriate personal information and images, photos and videos. Do not accept pupils or their parentsas friends on your personal profile. Do not accept ex-pupils as friends. Do not write / post indiscrete comments about colleagues or pupils and their families.
Webcams		
Ensure you know about inbuilt software / facilities and switch off when not in use.	Check the e-safety policy for any instances where using personal devices may be allowed.	Do not download images from school's equipment to your own. Do not use your own equipment without the permission of the Headteacher / Senior Leader. Do not retain, copy or distribute images for your own personal use.

Sexting / Peer on Peer Abuse / Cyberbullying

All staff should be aware that safeguarding issues can manifest themselves via peer on peer abuse. This could include cyberbullying and sexting. Staff should be clear as to the school policy and procedures with regards to peeron peer abuse. Further guidance on Sexting and Cyberbullying and how to handle incidents can be found below:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB_1_.PDF

https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Searching Devices, Viewing And Deleting Imagery

Adults should not view youth produced sexual imagery unless there is good a clear reason to do so. If the capture involves Child Abuse images (or suspected child abuse images):

- Do not print or copy images.
- Do not email a copy of the image to anybody.
- Do not show the image/capture to a minor.
- Do not show the image on the system to anybody who does not need to be exposed to the image.
- Ensure that the image/capture is saved in the Saved Capture area, for review, if required by those responsible for dealing with the issue.

Any printing, emailing or copying of a child abuse image is an offence under English Law. A child abuse image orindecent image of a child is an image of a sexual nature which depicts a child under the age of 18.

If the capture involves Adult pornography:

- Do not print out or copy images out unless necessary
- Do not email a copy of the image to anybody, unless necessary
- Do not show the image on the system to anybody who does not need to be exposed to the image.
- Ensure that the image/capture is saved in the 'Saved Capture' area, for review, if required by those responsible for dealing with the issue.
- Do not show the image/capture to a minor.

An offence against English law may be committed if adult pornography image is shown to a child. If there is a need to print out the image to show an adult this must be kept secure and not for general circulation.

Filtering and Monitoring

Governing Bodies and proprietors should be doing all that they reasonably can to limit children's exposure to therisks below in regards to online material:

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users; and
- conduct: personal online behaviour that increases the likelihood of, or causes harm.

As part of this process the school has appropriate filters and monitoring systems in place. The appropriateness of these filters will be considered and governors and proprietors will consider a whole school approach to online safety.

Governors and proprietors will ensure that staff to undergo regularly updated safeguarding training and that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

Information And Support

There is information available to support schools to keep children safe online. The following is not exhaustive:

www.thinkuknow.co.uk

www.disrespectnobody.co.uk

www.saferinternet.org.uk

www.internetmatters.org

www.childnet.com/cyberbullying-guidance

www.pshe-association.org.uk

educateagainsthate.com

www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Complaints

We will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school , the Academy Trust or the Local Authority can accept liability for material accessed, or any consequences of Internetaccess.

Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:

- Interview / counselling by teacher / Head of Year or Head of Faculty / Online Safety Coordinator / Headteacher;
- Informing parents or carers;
- Removal of Internet or computer access for a period, (which could ultimately prevent access to files held onthe system, including examination coursework);
- Referral to LA / Police.

Our Online Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Headteacher. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / Academy/ LA child protection procedures.