Moorlands Learning Trust

E-Safety Policy

	Position/Committee	Date
Prepared by	Trust IT Strategy Group	October 2022
Approved by	CEO	November 2022
To be Reviewed	CEO	November 2024

Contents

1. Aims 3
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating students about online safety 5
5. Educating parents about online safety 5
6. Social media contact with students 6
7. Cyber-bullying 6
8. Acceptable use of the internet in academies 7
9. Children and online safety away from the academy 7
10. Mobile technologies, including removable media devices 8
11. Student use of mobile technology 8
12. Use of digital and video images 9
13. Publishing student's images and work 9
14. Data protection 10
15. Clear screen 11
16. Managing the internet safely 11
17. Managing email 11
18. Unacceptable use 12
19. Misuses or infringements 12
19.1 Illegal incidents 13
20. Training 13
21. Complaints 14
22. Monitoring arrangements 14

Appendix 1 – Mobile Technologies 15
Appendix 2 – Managing the Internet Safely Guidance 17
Appendix 3 – Unacceptable Use 19
Appendix 4 – E-Safety Incident Log 21
Appendix 5 – How to deal with online safety incidents flow chart 22

1. Aims

At Moorlands Learning Trust, our academies aim to:

Have robust processes in place to ensure the online safety of students, staff, volunteers and governors.

Deliver an effective approach to online safety, which empowers us to protect and educate the whole academy community in their use of technology.

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Staff have a duty of care to protect children from risk of harm, as well as a duty to ensure their own conduct does not bring into question their suitability to work with children.

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance Keeping Children Safe in Education and its advice for academies on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996, the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which gave teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National curriculum computing programmes of study.

3. Roles and responsibilities

3.1 Trust Board and Local Governing Body (LGB)

Trustees, through the CEO, or Governors, where the academy has an LGB in place, have overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

3.2 The Headteacher/Principal

The Headteacher/Principal is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the academy.

3.3 The Designated Safeguarding Lead

Details of each academy's Designated Safeguarding Lead (DSL) and deputies are set out in the Trust's Child Protection and Safeguarding Policy.

The DSL takes lead responsibility for online safety in the academy; in particular:

Supporting the Headteacher/Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the academy.

Working with the Headteacher/Principal and other staff, as necessary, to address any online safety issues or incidents.

Ensuring that any online safety incidents are logged and dealt with appropriately, in line with this policy.

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with each academy's Anti-Bullying Policy.

Updating and delivering staff training on online safety.

Liaising with other agencies and/or external services if necessary.

Ensuring that E-Safety is taught to all students as part of the curriculum in line with guidance found in Section 4 of the E-Safety Policy.

This list is not intended to be exhaustive.

3.4 The role of the IT Support Department

The IT Support Department is responsible for:

Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at the academy, including terrorist and extremist material.

Ensuring that the academies' IT systems are secure and protected against viruses and malware and that such safety mechanisms are updated regularly.

Conducting a full security check and monitoring the academies' IT systems.

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

Working with the DSL as appropriate, ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the academy's Anti-Bullying Policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff and volunteers (including contractors and agency staff) are responsible for:

Maintaining an understanding of this policy (where relevant to their role).

Implementing this policy consistently.

Agreeing and adhering to the terms on acceptable use of the Academies' IT systems and the Internet, as per the Academy's IT Acceptable Use Policy.

Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately.

Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Academy's Anti-Bullying Policy.

Content on their own personal social media networks and electronic devices. This means that staff are responsible for managing their own applications and content to ensure that it does not breach this policy, or undermine public confidence in the school or the education profession.

Security and privacy settings when using social media via their chosen equipment. As such failing to ensure adequate and appropriate settings are in place may lead to disciplinary action should the content be found to breach Trust and Academy expectations of professional conduct and/or by bringing the school into disrepute.

Ensuring their own use of IT and social media is professional and appropriate at all times. Staff must be aware that their conduct online, both inside and outside of school, must not breach the Trust's Code of Conduct Policy or professional expectations. Any behaviour that is deemed to breach such expectations may be subject to disciplinary action.

Ensuring that when working remotely, staff follow guidelines as outlined in this Policy and any Remote or Blended Learning Policy in place at the Academy at the time.

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to notify a member of staff or the Headteacher of any concerns or queries regarding this policy.

Parents should notify the academy immediately if they have any concerns in relation to their child's online safety.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues? UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues

Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

3.7 Visitors and members of the community

Visitors and members of the community who use the academy's IT systems, Wifi or Internet will be made aware of this policy, when relevant, and be expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use, as per the Academy's IT Acceptable Use Policy.

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum.

In **Key Stage 3**, students will be taught to:

Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.

Recognise inappropriate content, contact and conduct and know how to report concerns.

Students in **Key Stage 4** will be taught:

To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.

How to report a range of concerns.

Students in **Key Stage 5** will develop their understanding of all aspects of online safety through the wider curriculum.

The safe use of social media and the Internet will also be covered in other subjects, including through Relationships, Sex and Health Education programmes where relevant.

The academies will use assemblies and other pastoral time to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

In order to make best use of the many educational and social benefits of new and emerging technologies, students need opportunities to use and explore the digital world. Online risks are posed more by behaviours and values than the technology itself.

The academies will raise parents' awareness of Internet safety in letters or other communications.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the relevant Headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

6. Social media contact with students

Staff must not establish or seek to establish social contact with students, for the purpose of securing a friendship or to pursue or strengthen a relationship, even if a student seeks to establish social contact themselves. This includes 'liking' or commenting on social media posts made by students.

If this occurs coincidentally, the member of staff should exercise their professional judgement in making a response and be aware that such social contact could be misconstrued.

Staff should alert the DSL or Headteacher of any such contact immediately.

All contact with students should be through appropriate channels at all times and should be within clear and explicit professional boundaries. This means staff should only contact students using school email / online accounts and regarding school matters.

Staff should not use, give, or be required to give, their personal details such as home or mobile number, social media identities or personal email addresses to students. Any member of staff found to be in contact with students through any of the above means, or any other unapproved method, without prior consent of the Headteacher/Principal/senior leader may be subject to disciplinary action.

Internal email and approved contact systems should only be used in accordance with Trust and Academy policies.

7. Cyber-bullying

7.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (Further information can be found in the Academy's Anti-bullying Policy).

7.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, academies will ensure that students understand what cyber-bullying is and what to do if they become aware of it happening to them or others. Academies will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. (Further details can be found in the Academy's Anti-bullying Policy).

7.3 Examining electronic devices

Trust and Academy staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or

Disrupt teaching, and/or

Break any of the academy rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the Senior Leadership Team to decide whether they should:

Delete that material, or

Retain it as evidence (of a criminal offence or a breach of academy discipline) and/or

Report it to the Police.

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the Trust Complaints Policy.

7.4 Cyber-bullying of staff

Staff in schools, as well as students, may become targets of cyberbullying. Staff should never retaliate or personally engage with cyberbullying incidents. They should report incidents appropriately and seek support.

Staff should report all incidents to the designated line manager or member of their school senior management team. The designated person will take responsibility for ensuring the person being bullied is supported, for investigating and managing the incident, and for contacting the police and Local Authority if appropriate.

For various reasons, staff may find it difficult to report to their line manager in the first instance. They may want additional support or advice. They should know they can seek advice and help from their Union, professional association or other support agencies such as Education Support Partnership.

8. Acceptable use of the internet in academies

All staff, students, volunteers and governors are expected to sign an agreement regarding the acceptable use of the Academy's IT systems and the Internet. Visitors will be expected to read and agree to the academy's terms on acceptable use if relevant.

Use of the academies' Internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

Academies will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure that they comply with the above.

(Further information is set out in the Academy's IT Acceptable Use Policy).

9. Children and online safety away from the academy

Where students are using digital technology away from school for the purposes of remote learning, the duty to ensure appropriate supervision is the responsibility of the child's parent/carer.

It is important that all staff who interact with children, including online, continue to look out for signs a child may be at risk. Any such concerns should be dealt with as per the Child Protection and Safeguarding Policy and where appropriate, referrals should still be made to children's Social Care and as required, the Police.

Online teaching should follow the same principles as set out in the Guidance for Safer Working Practice (including Covid-19 Addendum issued in April 2020) for those working with children and young people in education settings (National Safer Recruitment Consortium May 2019).

The academy will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

Below are some things to consider when delivering virtual lessons, especially where webcams are involved:

- Group tuition should be the norm. In cases where 1:1 tuition is essential, staff must seek formal agreement from a senior manager and the student's parent and ensure that this has been clearly communicated to all parties in advance of the session.
- Staff and students must wear suitable clothing, as should anyone else in the household.
- Where staff are working remotely, any technology used for communication should be in appropriate areas. Staff need to be mindful that backgrounds do not compromise personal confidentiality or breach the guiding principles of safer working practice guidance for staff working in educational settings.

- Our academies reserve the right for staff members to record live streamed sessions with students as a log of the activity. By joining the learning session parents give permission for this to happen.

- Recorded live sessions can be reviewed by the Academy if any issues were to arise.

- If live streams are to be recorded, this will be communicated clearly at the start of the session.

- Language must be professional and appropriate, including any family members in the background.

- Staff must only use platforms specified by senior managers and approved by our IT Network Manager / provider to communicate with students.

- Any recording of live sessions must be recorded through the Microsoft Teams function and only stored within a school OneDrive account

10. Mobile technologies, including portable media devices

Portable media devices, including laptops, ipads, mobile phones, tablets and USB memory sticks are particularly vulnerable to loss or theft due to their size and portability. This is especially true of those devices not owned or managed by the academy or Trust and any such devices must be encrypted or password protected as the default. (If you are in any doubt about the level of security that should be used for any media device then it is your responsibility to check this with IT Support).

Users must also take all reasonable precautions to prevent a security breach when using removable media devices and must **only** access or store work emails or files on these devices through the official Trust approved, secure applications (e.g. Microsoft Outlook, One Drive, ClassCharts) and not through any 3rd party / in-built apps – e.g. not through the inbuilt iphone Mail app or by downloading offline files to the device

Special care must be taken to physically protect the removable media device and stored information from loss, theft or damage. Anyone using removable media devices, especially those not owned or managed by the academy or Trust, to transfer information must consider the appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss as well as the security of any data stored on the device. For example, portable devices should not be left unattended or stored, even temporarily, in vehicles, to reduce the risk of theft.

Only information that is authorised and necessary to be transferred should be saved on to removable media devices. Users should note that the information that has been deleted can still be retrieved.

Removable media devices must not be used for archiving or storing records as an alternative to other academy or Trust approved storage equipment or systems

Further detailed guidance can be found in Appendix 1.

It should be noted that if a user loses or has a mobile device/tablet stolen which contains unencrypted personal data owned by Moorlands Learning Trust or its Academies, they may be liable to prosecution under the Data Protection Act 1998.

11. Student use of mobile technology

Students' use of mobile technology devices should only be used in line with individual academy policy.

If mobile devices (e.g. phones, ipads, tablets) are permitted within the academy, students must ensure that their usage adheres to the Acceptable Use Policy. Students must not:

- Use mobile technology to record or take photographs of one another or members of staff

- Ensure that all websites, apps or games accessed are age appropriate in line with the Acceptable Use Policy.

If a student chooses to bring a mobile phone on site, they remain the responsibility of the child. Moorlands Learning Trust and its Academies will accept no responsibility for the loss of students' personal mobile devices.

12. Use of digital and video images

- 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 they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

- With the appropriate written consent of parents (on behalf of students) and staff, academies may permit the appropriate taking of images by staff and students using academy equipment. When written consent is given, the academy may use the images on the website, the official academy's social media pages or for media and marketing purposes.

- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school/academy events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.

- **Staff** are not permitted to use personal digital equipment, such as mobile phones and cameras to record video or images of students; this includes on field trips. However, with the express advance permission of the Headteacher/Principal, images can be taken on personal devices, provided they are transferred immediately / at the earliest possible opportunity and solely to the Academy's/Trust's own network or cloud storage and deleted from the staff device.

- Care should be taken when taking digital/video images that students/students are appropriately dressed and are not participating in activities that might bring the individuals or the academy into disrepute.

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

- Photographs published on the website, or elsewhere, that include students will be selected carefully and will comply with good practice guidance on the use of such images.

- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs, unless there is specific authority from the Headteacher/Principal and / or the parent of the child concerned.

13. Publishing student's images and work

On a student's entry to the academy, parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the academy website

- On the academy's learning platform

- On social media platforms

- In the academy's prospectus and other printed publications that the academy may produce for promotional purposes

- Recorded / transmitted on a video or webcam

- In display material that may be used in the academy's communal areas
- In display material that may be used in external areas e.g. an exhibition promoting the academy; and
- General media appearances, e.g. local or national media/press releases sent to the press highlighting an activity (sent using the traditional methods or electronically).

The consent form is considered valid for the entire period the child attends the academy unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues etc.

Parents/carers may withdraw permission in writing, at any time. Consent has to be given by the person with parental responsibility to be valid.

Students' full names should not be published alongside their image. Email and postal addresses of students will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed. No photos should be uploaded to websites or other publications without prior checking with the Headteacher/Principal or nominated responsible person at the academy.

Only Moorlands Learning Trust or the nominated responsible person at the academy has authority to upload images to the site. If links to YouTube are provided a disclaimer must state that this link is to an external website and that the Moorlands Learning Trust is not responsible for the content of external sites.

14. Data protection

When personal data is stored on any mobile device or removable media the:

- data or device must be encrypted (check with IT Support if you are unsure about whether or not your device or data is encrypted)
- device must be password or pin protected
- device must be protected by up to date virus and malware checking software where applicable
- data must be permanently deleted from the device, in line with school/academy policy, once it has been transferred or its use is complete.

Staff must ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, whether on mobile or removable devices or not;
- can recognise a possible data breach, understand the need for urgency and know who to report it to within the Academy;
- can help data subjects (staff, students) understand their rights and know how to handle a data access request whether verbal or written and know who to pass it to in the Academy;
- where personal data is stored or transferred on mobile or other devices (including USBs) it must be ensured that either the data or the devices are encrypted, and password protected;
- will not transfer any Academy or Trust personal data to personal devices except as in line with Academy and Trust policy;
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

15. Clear screen

All users are expected to log off from their PCs/ laptops when left for long periods and overnight.

When leaving their desk e.g. for lunch or to attend a meeting, users should log off or lock their screen using Ctrl, Alt, Del and then selecting 'Lock Workstation'. Taking this measure will further reduce security risk. Staff should also ensure to lock their screens when leaving laptops unattended if working from home.

Mobile devices through which access to the network or cloud storage can be obtained, for example iPads and laptops, should be PIN / password protected, and set to lock after a period of no more than 5-10 minutes of inactivity and switched off when left unattended. These devices should be stored securely when not in use.

16. Managing the internet safely

Moorlands Learning Trust and its Academies monitor internet use from all computers and devices connected to the central network, as well as any devices where the internet filtering operates outside of the school network, including at home. For all traffic, the monitoring system records the source IP Address, the date, the time, and the destination site or server. Where possible, the system records the User ID of the person or account initiating the traffic.

IT Support members, and members of the Academy or Trust SLT, may access the records and data, if necessary, to respond to a security incident or as part of a live investigation sanctioned by the Headteacher/Principal or Trust. Further guidance on managing the Internet safely can be found in Appendix 2.

17. Managing email

The Moorlands Learning Trust email system must not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about any protected characteristic. Employees or students who receive any emails with this content from any Moorlands Learning Trust student or employee should report the matter to the Designated Safeguarding Lead immediately. Any breach of this E-Safety policy may be dealt with under the Moorlands Learning Trust Disciplinary Policy, up to and including the termination of employment for staff or the permanent exclusion of a student.

Sending chain letters or joke emails from a Moorlands Learning Trust email account is prohibited. Virus or other malware warnings and mass mailings from MLT accounts must be approved by IT Support before sending.

Staff and students at Moorlands Learning Trust shall have no expectation of privacy in anything they store, send or receive on the Trust or Academy's email system. Moorlands Learning Trust may monitor messages without prior notice.

Staff and students at Moorlands Learning Trust are provided with an Academy or Trust email account. Employees and students are not permitted to use personal email accounts for MLT / Academy business. Unless approved by an employee's Line Manager, MLT emails will not be automatically forwarded to an external email address.

18. Unacceptable use

The activities listed in Appendix 3 are prohibited.

19. Misuses or infringements

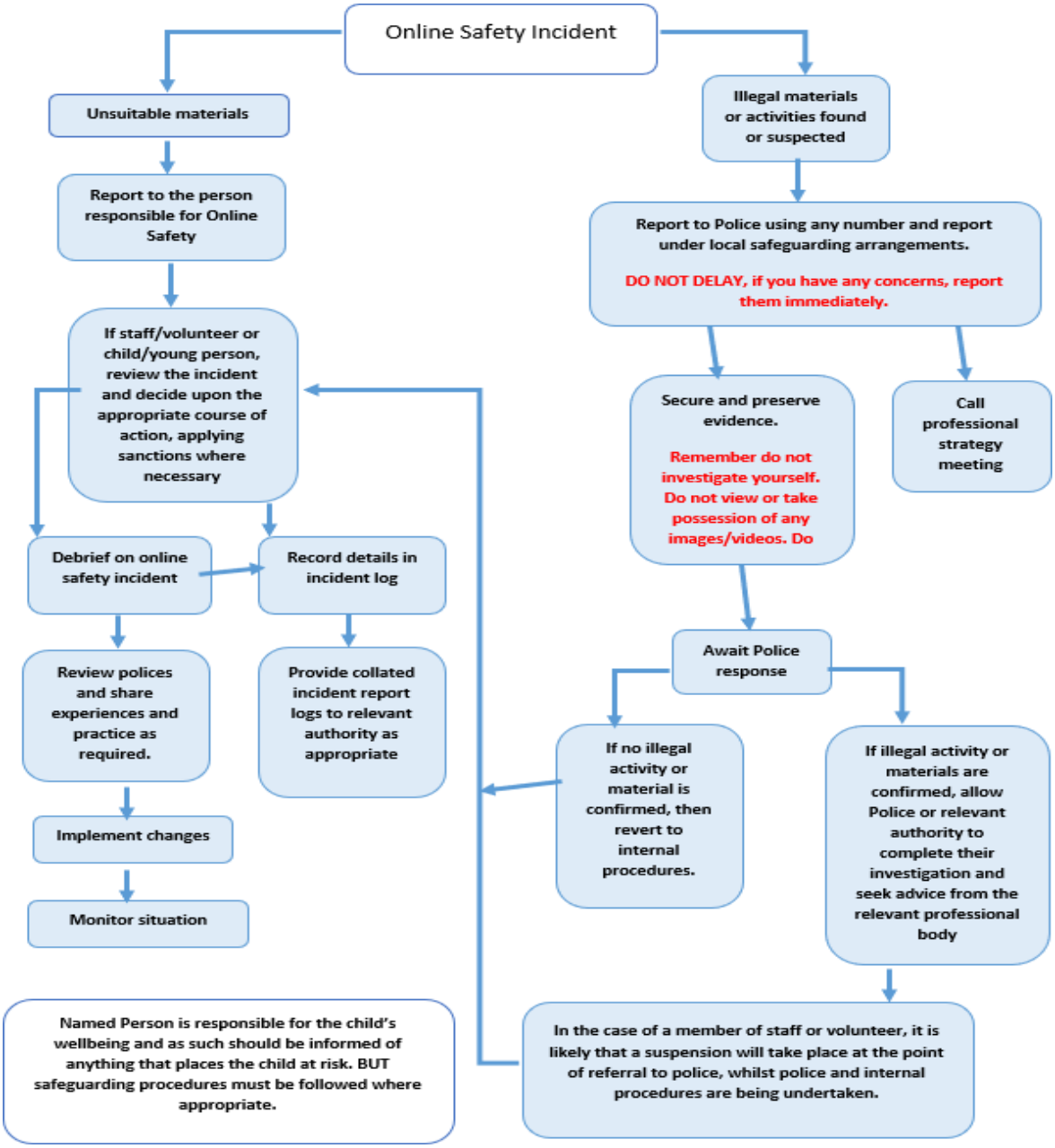
All users must be made aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Academy's Designated Safeguarding Lead. The Designated Safeguarding Lead or other appropriately designated members of staff, such as Heads of Year or Pastoral Managers, must record the incident on the e-safety log. Please see Appendix 4. This incident log must be monitored by the Headteacher/Principal or designated SLT member. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the Designated Safeguarding Lead. Depending on the seriousness of the offence further action taken may include:

- Investigation by the Headteacher/Principal or an appointed Investigating Officer
- Immediate sanctions, possibly leading to exclusion/dismissal; and/or
- Involvement with the police for very serious offences.

Users are made aware of the sanctions relating to the misuse or misconduct through inductions (staff) and IT lessons (students).

19.1 Illegal incidents

If there is any suspicion that the website(s) or social media platform concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and Appendix 5) for responding to online safety incidents and report immediately to the Police.



20. Training

As part of their ongoing professional development, all staff members will receive training regarding safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety. They will also update their knowledge and skills on the subject of online safety at regular intervals. The Designated Safeguarding Lead will keep a central record of evidence to prove all staff have completed annual training in these areas.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

21. Complaints

Complaints relating to E-Safety should be made to the academy's Designated Safeguarding Lead or Headteacher. E-safety incidents should be logged using the log in Appendix 4.

22. Monitoring arrangements

The DSL or other appropriately designated members of staff, such as Heads of Year or Pastoral Managers, will log behaviour and safeguarding issues related to online safety. N.B. The DSL should always be informed in line with normal safeguarding procedures where appropriate.

This policy will be reviewed every two years, or when there are changes to relevant legislation, by the DSL and senior colleagues involved in the e-safety curriculum design and IT Support.

Appendix 1 – Mobile / Portable Technologies

1. Laptops

In order to minimise the potential risks, users must apply the following security controls:

1.1 The physical security of laptops is the personal responsibility of users who must take all reasonable precautions, be sensible and stay alert to those risks.

1.2 Users must keep laptops within their possession, within sight wherever possible. They should never be left unattended in public view. Extra care should be taken in public places such as airports, railway stations or restaurants.

1.3 Where possible, laptops should be locked out of sight and must never be left unattended in a vehicle. If absolutely necessary, it should be locked out of sight in the boot, but it is generally safer for the user to take the device with them.

1.4 Laptops should be carried and stored in a padded laptop computer bag or strong briefcase to reduce the chance of accidental damage. (An ordinary-looking briefcase is also less likely to attract thieves than an obvious laptop bag.)

1.5 In the event of loss or theft the Police must be notified immediately and IT Support informed as soon as practically possible.

1.6 Information should not be stored on local hard drives unless there is no alternative. Protectively marked information must not be stored on the hard drive unless it is encrypted.

1.7 Data encryption will be applied to all laptop hard drives owned by the Moorlands Learning Trust by the 1st of January 2023

2. iPads, Tablets, mobile phones and USB Sticks

2.1 In order to minimise any potential risks, users must apply the following security controls:

2.1.1 Staff personal devices must not be connected to a laptop or desktop for any other purpose than re-charging the device.

2.1.2 No protectively marked or sensitive information may be stored on a mobile device unless the file or device is encrypted and the device is locked with a PIN code / password. This means that staff must **only** access or store work emails, files or data on these devices through the official Trust approved, secure applications (e.g. Microsoft Outlook, One Drive, ClassCharts) and not through any 3rd party / in-built apps – e.g. not through the inbuilt iphone Mail app or by downloading offline files to the device. It is the responsibility of the staff member to check the security / encryption levels required with IT Support if they are in any doubt.

2.1.3 It is the user's responsibility to ensure that sensitive information, including that contained in emails, is not to be held on a mobile device for longer than necessary.

2.1.4 The downloading of unauthorised apps and software on to a Moorlands Learning Trust device is prohibited.

2.1.5 Employees must report any suspected virus to IT Support immediately.

2.2 Employees must take all appropriate steps to protect the mobile device from loss, theft or damage. These steps include, but are not limited to:

2.2.1 The mobile device must not be left unattended in public view in a vehicle,

2.2.2 The mobile device must not be left unattended in a public place.

2.2.3 The keypad must be locked at all times when the mobile device is not in use.

2.2.4 All mobile devices must be password/pin protected.

2.2.5 Users should be aware that Moorlands Learning Trust may deploy software to monitor the use of removable media devices and the transfer of information to and from all removable media devices and MLT owned IT equipment. It may prohibit the use of devices that have not been recorded on the MLT IT Asset Register. Management reports may be generated and used to support internal and external audits.

2.2.6 Damaged, faulty or infected devices must not be used.

2.2.7 Up-to date virus and malware checking software must be operational where applicable on both the machine from which the information is taken and the machine on to which the data is to be loaded. (Check with IT Support if you are unsure about this for a personal mobile device)

2.2.8 If whilst using removable media the checking software indicates there is a problem, use of the device must be stopped immediately and IT Support informed so it can be recorded as an incident.

Appendix 2 – Managing the Internet Safely Guidance

1. Internet Use Filtering Systems

1.1 IT Support will block access to Internet websites and protocols that are deemed inappropriate for the MLT environment. The following protocols and categories of websites may be blocked for example:

1.1.1 Adult/sexually explicit material;
1.1.2 Advertisements and pop ups;
1.1.3 Chat and Instant messaging;
1.1.4 Gambling;
1.1.5 Hacking;
1.1.6 Illegal drugs;
1.1.7 Intimate apparel and swimwear;
1.1.8 Peer to peer file sharing;
1.1.9 Personals and dating;
1.1.10 Social network services;
1.1.11 SPAM, phishing and fraud;
1.1.12 Spyware;
1.1.13 Tasteless and offensive content;
1.1.14 Violence, intolerance or hate and
1.1.15 Certain, non-approved, web-based email.

2. Internet Use Filtering Exceptions

2.1 If a site is mis-categorised, employees may request the site be un-blocked by logging a ticket on the helpdesk. IT Support will review the request and un-block the site if it is mis-categorised. The DSL and / or the SLT e-Learning Lead should be consulted if there is any difference of opinion on categorisation.

2.2 Employees may access blocked sites with permission if access is appropriate and necessary for business purposes. If an employee needs access to a site that is blocked and appropriately categorised, they must discuss and obtain permission with a member of the senior leadership team who will communicate this in writing to IT Support.

3. Students

3.1 All students are advised to be cautious about the information given by others on sites, for example, users not being who they say they are.

3.2 Students should avoid placing images of themselves (or details within images that could give background details) on sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

3.3 Students are always reminded to avoid giving out personal details on sites which may identify them or where they are (full name, address, mobile number, academy details, email addresses, specific hobbies/interests, social media handle).

3.4 Students are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

3.5 Students are encouraged to be wary about publishing specific and detailed private thoughts online.

3.6 Our students are asked to report any incidents of bullying to a member of staff at the academy.

4. Employees

4.1 Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using systems approved by the Academy.

4.2 An individual is free to talk about Moorlands Learning Trust or their academy online. However, instances of MLT or an MLT academy and / or its staff being publicly criticised or brought into disrepute may constitute misconduct or gross misconduct and disciplinary action will be taken.

4.3 An employee must not disclose confidential information relating to their employment at Moorlands Learning Trust.

4.4 Sites must not be used to verbally abuse staff students or the Academy or MLT. Privacy and feelings of others should be respected at all times. Care should be taken to avoid using language which could be deemed as offensive to others.

4.5 If information on a site raises a concern with regard to conflict of interest, employees should raise the issue with their Line Manager / member of SLT.

4.6 If approached by a media contact about content on a site relating to Moorlands Learning Trust or an Academy, employees should advise their line manager before taking any action.

4.7 Viewing or updating personal sites must not take place during working time unless agreed in advance by your Line Manger.

4.8 Sites must not be used for accessing or sharing illegal content.

4.9 Blogging from the Moorlands Learning Trust systems is subject to monitoring.

Appendix 3 Unacceptable Use

Under no circumstances is an employee of Moorlands Learning Trust to engage in any activity that is illegal under UK or international law whilst utilising MLT resources. Failure to adhere to this may result in disciplinary action being taken in line with the MLT Disciplinary Policy.

The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

1. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Moorlands Learning Trust.

1.2 Unauthorised copying of copyright material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Moorlands Learning Trust or the end user does not have an active licence.

1.3 Exporting software, technical information, encryption software or technology, in violation of internal or regional export control laws, is illegal. Advice should be sought prior to export of any material that is in question.

1.4 Introduction of malicious programmes into the network or server (e.g. viruses, worms, Trojan horses, e-mail bombs, etc).

1.5 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

1.6 Using a Moorlands Learning Trust computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

1.7 Making fraudulent offers of products, items or services from any Moorlands Learning Trust account.

1.8 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a sever or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purpose of this section, “disruption” includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

1.9 Port scanning or security scanning is expressly prohibited unless prior notification to Moorlands Learning Trust is made.

1.10 Executing any form of network monitoring which will intercept data not intended for the employee’s host unless this activity is part of the employee’s normal job/duty.

1.11 Circumventing user authentication or security of any host, network or account.

1.12 Interfering with or denying service to any user other than the employee’s host (for example, denial of service attack).

1.13 Using any programme/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user’s terminal session, via any means, locally or via the Internet/Intranet/Extranet.

1.14 Providing information about, or lists of, Moorlands Learning Trust’s employees to outside partners.

2. Email and Communications Activities

The following activities are strictly prohibited, with no exceptions:

2.1 Sending unsolicited email messages, including the sending of “junk mail” or other advertising material to individuals who did not specifically request such material (email spam).

2.2 Any form of harassment via email, telephone, social media or other means, whether through language, frequency, or size of messages.

2.3 Unauthorised use, or forging, of email header / footer information.

2.4 Solicitation of email for any other email address, other than that of the poster’s account, with the intent to harass or to collect replies.

2.5 Use of unsolicited emails originating from within Moorlands Learning Trust’s networks of other Internet/Intranet/Extranet service provides on behalf of, or to advertise, any service hosted by MLT or connected via the MLT network.

Employees may be excepted from these restrictions during the course of their legitimate job responsibilities (e.g. systems administration staff may need to disable the network access of a host if that host is disrupting production services). Any exception must be approved by your Line Manager before it is used.

2.6 The automatic forwarding of Moorlands Learning Trust emails to email addresses or accounts outside the Trust.

Appendix 4 – E-Safety Incident Log

Details of all E-Safety incidents must be recorded by the Designated Safeguarding Leads using the E-Safety log below or within CPOMS. This incident log will be monitored termly by the Headteacher or designated member of the Academy's SLT.

Date and Time	Name of Pupil or Staff Member	Male/Female	Room and Computer/ Device Number	Details of Incident (including evidence)	Actions and Reasons

Appendix 5 – How to deal with online safety incidents flow chart