Online Safety Policy

March 2024

Document type	Published online and available to all staff
Last revision date	March 2024
Next revision date	March 2026
Owner	Group IT Services Manager
Authors	Group IT Services Manager
Version	2.0
Status	Approved at Audit Finance and Risk Committee – February 2024

Contents

This policy applies to:

All Trust settings and any school converting into the trust since the last review and approval of this policy.
Where this policy states 'school' this means any of our educational establishments and the wider Trust.
Where this policy states 'Headteacher' this also includes 'Head of School' and 'Centre Manager'.
Mowbray Education Trust (MET).

1. Aims

Being online has become an integral part of life. Social media, online games, websites and apps can be accessed through mobile phones, computers, laptops and tablets – all of which form a part of the online world.

The internet and online technology provide new opportunities to learning and growth, but it can also expose new types of risks.

Employees are likely to be subjected to a higher level of public scrutiny over and above other public sector employees due to their work with children and vulnerable persons and do so generally without encountering any difficulty.

This policy aims to:

- Set guidelines, rules, and clear expectations for Online Safety
- Prevent disruption to the school arising from the misuse of Online services

2. Relevant legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance Keeping Children Safe in Education refers to, and complies with, the following legislation and guidance:

- Education Act 2011
- The Education and Inspections Act 2006
- Equality Act 2010
- Teaching online safety in schools
- Preventing and tackling bullying
- cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation
- Protecting children from radicalisation

3. Definitions

- **"ICT systems"**: includes all technology, facilities, systems and services including but not limited to desktops, laptops, desk phones, mobile phones, wearable technology and other computer-based hardware and software.

- "**Users**": anyone who uses ICT systems, including governance volunteers, staff, parents, pupils,

volunteers, contractors, and visitors.

- "**Personal use**": any use or activity not directly related to the users' employment, study, or purpose.

- "**Authorised personnel**": employees authorised by the school to perform systems administration and/or monitoring.

- "**Content**": files and data including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

4. Roles and Responsibilities

4.4. The Trust Board

4.4.1. Monitoring this policy and holding the Headteacher to account for its implementation.

4.4.2. Should ensure that they are familiar with the contents of this policy and its relationship to the school's standards, policies, and guidance on the acceptable use of ICT and e-safety.

4.4.3. Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3).

4.5. Headteacher

4.5.1. Ensure that all users are trained and become familiar with this policy and its relationship to the school's standards, policies, and guidance on the acceptable use of ICT and e-safety.

4.5.2. Provide opportunities to discuss appropriate ICT systems use on a regular basis and ensure that any queries raised are resolved swiftly.

4.5.3. Must ensure that any allegations raised in respect of ICT systems are investigated promptly and appropriately, in accordance with the school's disciplinary procedure, code of conduct and acceptable use policy.

4.6. Designated Safeguarding Lead (DSL)

4.6.1. Takes lead responsibility for online safety in school.

4.6.2. Support the headteacher in ensuring that users understand this policy and that it is being implemented consistently throughout the school.

4.6.3. Work with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.

4.6.4. Ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.

4.6.5. Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.

4.6.6. Update and deliver user training on online safety (appendix 4 contains a self-audit for staff on online safety training needs).

4.6.7. Liaise with other agencies and/or external services if necessary.

4.6.8. Provide regular reports on online safety in school to the headteacher and/or trust board(or delegated committee).

This list is not intended to be exhaustive.

4.7 The ICT manager

4.7.1. Put in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep users safe from potentially harmful and inappropriate content online while at school, including terrorist and extremist material.

4.7.2. Ensure that school's ICT systems are secure and protected against viruses, malware and are updated regularly

4.7.3. Block access to potentially dangerous content, and where possible, prevent the download of potentially dangerous content.

4.7.4. Ensure that any online safety incidents are logged (See appendix 5) and dealt with appropriately in line with this policy.

4.7.5. Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

4.8 Users

4.8.1. Maintain an understanding of this policy.

4.8.2. Implement this policy consistently.

4.8.3. Agree and adhere to the terms on the acceptable use of School's ICT and internet acceptable use policy.

4.8.4. Work with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.

4.8.5. Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

4.9 Parent/Carer

4.9.1. Notify a member of staff or the headteacher of any concerns or queries regarding this policy.

4.9.2. Ensure their child has read, understood and agree to the terms on acceptable use of school's ICT systems.

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

- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent factsheet - Childnet International

5. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and

contact In **Key Stage 3**, pupils 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 Pupils 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

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

6. Educating Parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website.

Online safety will also be covered during parents' evenings.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

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

7. Cyber-bullying

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.

7.1. Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers/form teachers will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governance volunteers and volunteers (where appropriate) receive training on cyber- bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

8. Examining electrical devices

School 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 pupils' 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 school 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 school discipline), and/or
- Report it to the police

Any searching of pupils 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 pupils' electronic devices will be dealt with through the school complaints procedure.

9. Acceptable use of the internet in school

All users are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3).

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

We will monitor the websites visited to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

10. Pupils using mobile devices and wearable technologies in school

Primary

Year 5 and 6 pupils who walk to school are permitted to bring mobile phones to school with them.

Once on site they must deposit with designated staff members for safe keeping until the end of the day where they can be collected to take home with them.

Secondary

Are **NOT** allowed to be seen or used on site at any point during the day, this includes break and lunchtime and outside the building.

Students may have their phone with them, but it is to be turned off and in their bag, not in a pocket of any item of their clothing or coat.

Wearable technologies are **NOT** allowed to be worn in school.

Mobile phone or wearable technology which contravene this policy will be confiscated, logged on class charts and locked away.

They will be returned to parent/carer by arrangement at the convenience of the leadership team – likely to be 3.30 Friday.

11. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3 and the ICT and internet acceptable use policy.

Staff must ensure that their work device is secure and protected with biometrics or password, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager. Work devices must be used solely for work activities.

12. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

13. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy/deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governance volunteers will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every 2 years by the ICT Manager. At every review, the policy will be shared with the Audit, Finance and Risk Committee.

15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Social media policy

Log of Changes to Document

Version	Date	Page	Change	Approver:
V1.0	Oct-19	All pages	New policy created for CEO approval	Group Operations Manager
V1.0	TBC	All Pages	Draft for Approval	CEO
V2.00	Mar-22		3.0 definitions added 10.0 pupil mobile phone usage rulings added.	BOARD
V2.0	Mar 24	All pages	No changes to be made	Audit Finance and Risk committee

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I click on a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• I will be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends.
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	
I will read and follow the rules in the acceptable use agreement policy **When I use the school's ICT systems (like computers) and get onto the internet in school I will:** • Always use the school's ICT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my username and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others • Always log off or shut down a computer when I'm finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.**	
Signed (pupil):	**Date:**
Parent/carer's agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: acceptable use agreement (staff, governance volunteers, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNANACE VOLUNTEERS, VOLUNTEERS AND VISITORS	
Name of staff member/governance volunteer/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and/or biometric password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (staff member/governance volunteer/volunteer/visitor):	**Date:**

Appendix 4: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governance volunteers and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**