Manchester
Hospital School

E-Safety Policy

Document Control	
Title	E-Safety Policy
Policy Number	MHS050
Date	3rd March 2025
Supersedes	15th February 2023
Purpose of the policy	The purpose of this policy is to: ● Safeguard and protect all members of the school's community online ● Identify approaches to educate and raise awareness of online safety throughout the community ● Enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology ● Identify clear procedures to use when responding to online safety concerns.
Related policies/guidance	This policy links with a number of other policies, including: ● Information Security and Data Protection Policy ● Safeguarding and Child Protection Policy ● Staff Code of Conduct ● Acceptable Use Agreements for staff and pupils ● Behaviour Policy ● Anti-Bullying Policy
Review	Every 2 Years
Author	Gwen Rees-Moffitt
Date Consultation Completed	March 2025
Date adopted by	**FGB - 26th March 2025**

Under the Public Sector Equality Duty, Manchester Hospital School has due regard to the need to eliminate discrimination, harassment and victimisation and any other conduct prohibited by the Equality Act 2010; to advance equality of opportunity between those who share a relevant protected characteristic and those who do not share it and to foster good relations across all protected characteristics. Manchester Hospital School will take into account equality considerations when policies are being developed, adopted and implemented.

Manchester Hospital School serves the needs of a very large and diverse range of children, young people and their families at times when they are extremely vulnerable. Our core purpose as a school is to uphold the child's right to Education and our policies and procedures are necessary to keep staff and children safe . We acknowledge that our pupils are often living with a range of very complex medical conditions including mental ill health and therefore we keep the needs of the pupil at the heart of all decisions. We will , therefore, work within the parameters of all statutory policies whilst seeking to understand and support the child's long term education and health needs.

CONTENTS

1. Policy Introduction and Aims

The internet and associated devices, such as computers, tablets, mobile phones, games consoles and smart watches are an important part of everyday life. However, these modern technologies have created a landscape of challenges and dangers that is still constantly changing. In order to ensure that the school provides a safe environment for learning, we adhere to the following principles:

Online safety is an essential part of safeguarding and the school has a duty to ensure that all pupils and staff are protected from potential harm online
Online safety education is an important preparation for life. Pupils should be empowered to build resilience and to develop strategies to prevent, manage and respond to risk online.

The purpose of the online safety policy is to:

- Safeguard and protect all members of the school's community online
- Identify approaches to educate and raise awareness of online safety throughout the community
- Enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology
- Identify clear procedures to use when responding to online safety concerns.

The issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:

Content: being exposed to illegal, inappropriate or harmful material; for example pornography, racist or radical and extremist views, and in some respects fake news

Contact: being subjected to harmful online interaction with other users; for example children can be contacted by bullies or people who groom or seek to abuse them

Commercial exploitation: for example young people can be unaware of hidden costs and advertising in apps, games and website

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying

Furthermore, in recent years a change in the online landscape has allowed for greater opportunity for illegal activity and has created greater vulnerability for young people from the following risks:

- Sexual exploitation
- Identity theft
- Phishing
- Ransomware
- Spam
- 'Cyber' bullying / trolling
- Viruses
- Grooming

The rise in the use of Artificial Intelligence (AI) has also meant that computer programmes and ‘bots’ are able to mimic the language skills of human interaction. These bots have a huge scope for reaching millions of people and targeting a greater number of vulnerable young people for purposes of illegal activity.

2. Policy Scope

This policy applies to all staff including teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the school (collectively referred to as ‘staff' in this policy) as well as pupils and parents/carers. It applies to the whole school including the Early Years Foundation Stage. It applies to access to school systems, the internet and the use of technology, using devices provided by the school or personal devices.

The policy also applies to online safety behaviour such as cyber-bullying, which may take place outside the school, but is linked to membership of the school. The school will deal with such behaviour within this policy and associated behaviour and discipline policies, and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school.

2. Links with other policies and practices

This policy links with a number of other policies, including:

Data Protection Policy
Safeguarding and Child Protection Policy
Staff Code of Conduct
Acceptable Use Agreements for staff and pupils
Behaviour Policy
Anti-Bullying Policy

3. Roles and Responsibilities

Gwen Rees-Moffitt (Deputy Headteacher) is the Whole School Designated Safeguarding Lead (DSL) and Joanna Beswick (Headteacher) is the Whole School Deputy Safeguarding Lead; they are responsible for safeguarding. All school sites have a DSL who takes responsibility for child protection and safeguarding at their site. E safety is a key element of keeping children safe. All members of the community have important roles and responsibilities to play with regard to online safety:

3.1 The Head:

- Has overall responsibility for Safeguarding
- Ensures that online safety is viewed as a safeguarding issue and that practice is in line with national recommendations and requirements.
- Ensures the school follows policies and practices regarding online safety (including the Acceptable Use Agreements), information security and data protection
- Ensures that online safety is embedded within the whole school curriculum, which enables all pupils to develop an age-appropriate understanding of online safety

3.2 The Whole-School Safeguarding Lead:

- Supports the site DSLs by ensuring they have sufficient training, time, support and resources to fulfil their responsibilities
- Ensures that all staff receive regular, up to date and appropriate online safety training

- Is aware of what to do in the event of a serious online safety incident, and will ensure that there are robust reporting channels for online safety concerns, including internal, local and national support
- Monitor the online safety practice regularly in order to identify strengths and areas for improvement - including the monitoring and filtering of school devices (Securly)

3.3 The Whole-School Safeguarding Lead and site DSLs work together to carry-out the E-safety policy:

Whole School DSL:	● Promotes an awareness of and commitment to online safety throughout the school community ● Acts as the named point of contact for the school on all whole school online safety issues, and liaises with other members of staff or other agencies, as appropriate ● Facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate ● Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident ● Monitors Securly - our monitoring and filtering IT package ● Reports regularly to the Governors and SLT on monitoring and filtering effectiveness
Site DSL	● Takes day to day responsibility for online safety at their site ● Acts as the named point of contact on all online safety issues at their site, and liaises with other members of staff or other agencies, as appropriate ● Facilitates training and advice for all staff, keeping colleagues informed of current research, legislation and trends regarding online safety and communicating this to the school community, as appropriate ● Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident at their site

3.3 Staff managing the technical environment:

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internal use of the school's network is monitored and filtered to allow any inappropriate use to be identified and followed up.

Manchester Hospital School is aware of its responsibility when monitoring staff and pupil communication under current legislation and take into account:

- Data Protection Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Regulation of Investigatory Powers Act 2000
- Human Rights Act 1998
- General Data Protection Regulation 2018

The school will use Securly for monitoring and filtering activity on its network.

3.4 Managing the internet

All access to the school's WIFI will be monitored and filtered. All school devices will be monitored and filtered. Staff will make every effort to preview sites before recommending them to pupils; it is recognised that the content on internet sites is beyond the control of the school.

All users, staff and pupils, must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources. All users, staff and pupils, should make all reasonable attempts to observe copyright of materials from electronic resources.

All users, staff and pupils, must not post personal, sensitive, confidential or classified information, or disseminate such information in any way that may compromise its intended restricted audience while using the school's WIFI or school-managed devices.

All users, staff and pupils, must not reveal personal information about members of the school community (including names) on any social networking site or blog without seeking the subject's permission.

3.4 All school staff:

All staff should read, adhere to and help promote the E-safety policy, Acceptable Use Agreements and other relevant school policies and guidance.

All staff should take responsibility for the security of school systems and the data they use, or have access to.

All staff should model safe, responsible and professional behaviours in their own use of technology.

All staff should supervise, guide and monitor pupils carefully when engaged in activities involving online technology / lessons involving internet use.

All staff should have an up to date awareness of a range of online safety issues and how they may be experienced by the children in their care.

All staff should identify online safety concerns and take appropriate action by reporting to the DSL as soon as the problem emerges.

All staff should know when and how to escalate online safety issues.

All staff should take personal responsibility for professional development in this area and keeping up to date with technical advances which may pose a risk for young people.

3.5 Pupils (at a level that is appropriate to their individual age, ability and vulnerabilities):

All pupils should engage in age appropriate online safety education opportunities.

All pupils should read and adhere to the school Acceptable Use Agreements.

All pupils should respect the feelings and rights of others both on and offline, in and out of school.

All pupils should take responsibility for keeping themselves and others safe online.

All pupils should report to a trusted adult, if there is a concern online.

3.6 Parents and carers are encouraged to:

- Read the school Acceptable Use Agreements and encourage their children to adhere to them.
- Support the school in online safety approaches by discussing online safety issues with their children and reinforcing appropriate, safe online behaviours at home.
- Model safe and appropriate use of technology and social media, including seeking permission before taking and sharing digital images of pupils other than their own children.
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Use school systems and resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement

5.1 Education and engagement with pupils

The school curriculum includes age-appropriate lessons and activities on online safety for all pupils, intended to raise awareness, build resilience and promote safe and responsible internet use by:

- Ensuring education regarding safe and responsible use precedes internet access

Including online safety across the curriculum, including the Personal Social and Health Education, Relationships and Sex Education and Computing programmes of study, covering use both at school and home.

- Reinforcing online safety messages whenever technology or the internet is in use.
- Ensuring that the needs of our pupils who are all considered to be more vulnerable online, are met appropriately.
- Educating pupils in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
- Teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Teaching pupils to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Supporting pupils in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

5.2 Training and engagement with staff

The school will:

- Provide and discuss the Online Safety Policy and staff Acceptable Use Agreement with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
- Make staff aware that school systems are monitored and activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with school’s policies when accessing school systems and devices.
- Make staff aware that their online conduct out of school, including personal use of social media, could have an impact on their professional role and reputation within school.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting pupils, colleagues or other members of the school community.

5.3 Awareness and engagement with parents and carers

Parents and carers have an essential role to play in enabling children to become safe and responsible users of the internet and associated technologies. The school will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats
- Drawing parents' attention to the school online safety policy and expectations in newsletters and on the website.
- Requiring parents to read the pupil Acceptable Use Agreement and discuss its implications with their children.

6. Reducing Online Risks

The internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. The school will:

- Regularly review the methods used to identify, assess and minimise online risks.
- Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in school is permitted.
- Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
- Ensure, through online safety education and the school Acceptable Use Agreements, that pupils know that the school's expectations regarding safe and appropriate behaviour online apply whether the school's networks are used or not.

7. Safer Use of Technology

7.1 Classroom Use

The school uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Learning platforms
- Cloud services and storage
- Email and messaging

- Mobile phones
- Games consoles and other games based technologies
- Digital cameras, web cams and video cameras

Supervision of pupils will be appropriate to their age and ability.

All devices should be used in accordance with the school’s Acceptable Use Agreements and with appropriate safety and security measures in place.

Members of staff should always check websites thoroughly, and tools and apps for suitability before use in the classroom or recommending for use at home.

Staff and pupils should consider copyright law before using internet-derived materials by staff (and pupils should, where appropriate, comply with license terms and/or acknowledge the source of information).

7.2 Filtering and Monitoring

On our school network, all incoming data is screened by an application that provides real-time filtering and protects both networks and users from internet threats - the provider we use is Securly. It prevents a wide range of unwelcome material and malware from being available in school while at the same time allowing access to material of educational value. The policy determining filtering is managed centrally, with different levels being applied depending on adults or pupils.

The Securly system logs all internet access on MHS devices and any device connected to the school WIFI. These logs can be accessed by the whole school DSL for monitoring purposes. Flagged terms will also trigger alerts which are sent to the Whole School DSL as email alerts in real-time. Concerns identified will be managed according to the nature of the issue and screened by the Whole School DSL. A weekly report is generated by Securly which captures the activity which has been blocked during the week. The Whole School DSL monitors this to identify any users who are demonstrating online behaviours which are triggering Securly’s filter frequently. These users may need support with their internet habits or usage.

Securly monitors all email communications on the WIFI and all documents on the Google Drive.

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

All users are informed that use of school systems is monitored and that all monitoring is in line with data protection, human rights and privacy legislation.

7.3 Managing Personal Data Online

Personal data will be recorded, processed, transferred and made available online in accordance with the General Data Protection Regulations. Full information can be found in the school's Data Protection Policy.

8. Social Media

8.1 Expectations

The term social media includes social networking sites. The most common of these include:

- Instagram.
- YouTube.
- Facebook.
- X
- TikTok.
- Pinterest.
- Snapchat.
- LinkedIn.

It is important to note that new social media networking sites are being created all of the time and young people may have more knowledge about these sites than staff or parents/carers.

All members of the school community are expected to engage in social media in a positive, safe and responsible manner, at all times. Any activity which impacts on the reputation of the school will be dealt with by the Headteacher. This is detailed in the Staff Code of Conduct document.

8.2 Staff Use of Social Media

Safe and professional behaviour is outlined for all members of staff as part of the staff Code of Conduct, Staff Acceptable Use Agreement; this includes behaviour on social media networking sites.

Key members of school staff are responsible for the upkeep and maintenance of the school's official social networking sites.

8.3 Pupils' Personal Use of Social Media

Safe and appropriate use of social media will be taught to pupils as part of online safety education.

The school is aware that many popular social media sites state that they are not for children under the age of 13 years.

Inappropriate use of social media during school hours or whilst using school devices may result in removal of internet facilities or school devices. The site DSL will work with pupils to prevent further inappropriate use of the internet.

Any concerns regarding pupils' use of social media, both at home and at school, will be dealt with in accordance with existing school policies. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

9. Use of Personal Devices and Mobile Phones

The school recognises that personal communication through mobile technologies is an accepted part of everyday life for pupils, staff and parents/carers, but technologies need to be used safely and appropriately within school.

9.1 Expectations

All use of personal devices and mobile phones will take place in accordance with the law and other appropriate school policies, including, but not limited to: Anti-Bullying, Behaviour and Discipline, and Safeguarding and Child Protection.
Electronic devices of any kind that are brought onto site are the responsibility of the user at all times. The school accepts no responsibilities for the loss, theft, damage or breach of security of such items on school premises.

The sending of abusive or inappropriate messages/content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt according to the behaviour policy.

All members of the community are advised to ensure that their mobile phones and personal devices do not contain any content which may be considered to be offensive, derogatory or would otherwise contravene the school behaviour or Safeguarding and Child Protection policies.

Under no circumstances does the school allow a member of staff to use their personal mobile phone to contact a pupil. Staff are advised not to contact a Parent / Carer using their personal mobile phone but there may be circumstances concerning a duty of care to pupils which override this. In these cases staff are advised to block their number, prior to making the call using 141.

9.2 Staff Use of Personal Devices and Mobile Phones

Members of staff will ensure that the use of personal phones and devices takes place in accordance with the law, as well as relevant school policy and procedures, such as: Confidentiality, Safeguarding and Child Protection, Data Security and Acceptable Use Agreements.

Images of pupils must not be stored on personal devices.

9.3 Pupils' Use of Personal Devices and Mobile Phones

Pupils will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

Parents are advised to contact their child via the school reception during school hours.

Mobile phones should not be used by pupils during lessons unless as part of an approved and directed curriculum based activity with consent from a member of staff.

Mobile phones and personal devices (such as smart watches and bluetooth headphones) must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's grade in that examination or all examinations being nullified.

9.4 Visitors' Use of Personal Devices and Mobile Phones

Parents, carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with the school's Acceptable use Agreement and other associated policies, such as Anti-Bullying and Safeguarding and Child Protection policies.
The school will ensure appropriate and information is provided to inform parents, carers and visitors of expectations of use.
Members of staff are expected to challenge visitors if they have concerns and will always inform the site DSL of any breaches of school policy.

10. Responding to Online Safety Incidents and Concerns

All members of the school community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), sexual abuse as a result of online grooming, cyberbullying and illegal content.
All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns.
Incidents will be managed depending on their nature and severity, according to the relevant school policies.
After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes in policy or practice as required.
If the school is unsure how to proceed with an incident or concern, the site DSL will seek advice.
Where there is suspicion that illegal activity has taken place, the school will contact the Police using 101, or 999 if there is immediate danger or risk of harm.
If an incident or concern needs to be passed beyond the school community (for example if other local schools are involved or the public may be at risk), the school will speak with the Police and/or the Local Authority first, to ensure that potential investigations are not compromised.

10.1 Concerns about Pupils' Welfare

The site DSL must be informed immediately of any online safety incident that could be considered a safeguarding or child protection concern.
The site DSL will ensure that online safeguarding concerns are escalated and reported to relevant agencies.
The school will inform parents and carers of any incidents or concerns involving their child, as and when required.

11. Misuse

Complaints about IT misuse by pupils will be dealt with by the site lead under the relevant policies and procedures and according to the nature of the complaint.
Any complaint about staff misuse must be referred to the Headteacher.
Pupils and parents are informed of the school's complaints procedure via the school website.

11.1 Misuse of Digital images and video

Digital images are easy to capture, reproduce and publish and, therefore, misuse. It is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. With the written consent of parents /carers (on behalf of pupils), the school permits the appropriate taking of images by staff. Staff should only take photographs or videos of pupils with the express permission of pupil and parent/carer. This is normally obtained from parents/carers on admission to the school, but pupils / parents must always be asked for consent at the time of the photography capture as opinions can change.

It is preferred that school equipment is used for this, but in any other unique case, images must be transferred within a reasonable time scale and solely to the school's network or hosted services controlled by the school and (double) deleted from the original device. Pupils must be advised when using their personal digital equipment, especially during school trips, that images and video should only be taken with the subjects' consent. Pupils should also be advised that complaints against this condition will be considered a serious breach of this policy and risk having the device confiscated until it can be investigated by the site DSL and Whole-School Designated Safeguarding Lead.

Video Conferencing (Use of Google Meet)

No part of any video conference is to be recorded in any medium without the consent of those taking part.
Any remote learning will take place via Google Meet only, where only participants with a Manchester Hospital School email address can attend. Teachers and pupils must then adhere to remote learning guidance given on the Acceptable Use Agreement.

11.1 Monitoring and Review

The school will monitor and filter internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied in practice.
The policy framework will be reviewed at least annually, and in response to any new national guidance or legislation, significant developments in the use of technology, emerging threats or incidents that have taken place.

12. Useful links and sources of advice

Websites offering help and advice:
http://www.anti-bullyingalliance.org.uk
http://www.itgovernance.co.uk
http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml
http://www.thinkuknow.co.uk
http://www.ceop.gov.uk/
http://www.getsafeonline.org/
http://www.kidsmart.org.uk/