Meadowhead School and Sixth Form

Online Safety Policy

This is a policy of Meadowhead School and Sixth Form.

Staff Responsible:	Geoff Dearman – Assistant Headteacher
Author:	Geoff Dearman – Assistant Headteacher
Date of last review:	September 2025
Approval date:	4th September 2025
Date of next review:	September 2026

Online Safety Policy

Safeguarding children & young people online involves a range of issues e.g. cyberbullying, pressure to look 'right' & get 'likes', fake news, violence, extremist behaviour, grooming, child sexual & criminal exploitation, gambling and sharing semi/nude images.

Meadowhead School aims to educate pupils, parents, carers & staff about the benefits and risks of using this environment and provide safeguards and awareness for students to safely control their online experiences.

Our online safety policy has been developed based on guidance from Sheffield City Council Safeguarding Children Partnership, and appendix 1 is the Local Authority guidance and risk assessment, which the school also follows.

This policy will be monitored annually by the Online-Safety Coordinator. Any incidents, training outcomes, and updates in legal guidance will be used to inform changes.

All staff will receive annual online safety training, with updates provided in response to emerging threats or guidance. New staff are trained as part of induction.

The school uses Sophos XG ensuring compliance with UK Safer Internet Centre standards. This is an effective filtering and monitoring system that enables the school to safeguard pupils from harmful and inappropriate online material. Filtering and monitoring arrangements are designed to address known and emerging online risks, including cyberbullying, exploitation, radicalisation, misinformation, disinformation, conspiracy theories, deepfakes, and risks arising from the use of generative AI.

The school will ensure:

- A safe & secure network & broadband connection
- Compliant Information Communication Technology (ICT) security e.g. firewalls, access restrictions
- Online-safety policies are understood, implemented, reviewed by staff, pupils, parents & carers
- Staff, pupils, parents/carers use ICT responsibly
- A progressive, inclusive online-safety curriculum
- Relationships, Sexual Health Education (RSHE) includes online-safety issues

The school also has:

- A trained Online-Safety Coordinator who is the Designated Safeguarding Lead
- This Online-Safety Policy reflects our whole-school approach (above) including:
  - Using mobile devices, social media, smart technology
  - Acceptable ICT use for staff & pupils
  - Pupil and staff behaviour including bullying
  - Data protection, information sharing & security
  - Filtering and monitoring
  - Safe home-learning for pupils & staff

Our Online Safety Coordinator is Mr Geoff Dearman and he is responsible for:

- Undertaking SCSP Online-Safety Training
- Safeguarding students online and assessing the needs of students who may be at risk
- Supporting, training, educating staff/parents/carers
- Responsibility for filtering and monitoring systems oversight rests with the Governing Body, delegated to the Designated Safeguarding Lead (DSL) - Geoff Dearman and the Network manager. Further actions also include:
    - Filtering systems are reviewed at least annually and after any safeguarding incident.
    - Monitoring reports are reviewed termly by the DSL and shared with senior leaders.
    - Any identified risks are escalated immediately in line with safeguarding procedures.
    - Governors will receive annual training on filtering and monitoring responsibilities to ensure compliance with statutory duties from the DSL.

Meadowhead School will communicate information with students, staff, parents and carers including:

- Rules for online-safety & internet access in all areas of the school
- Articles about online-safety in our newsletters, publicity, website etc.

Students, staff, parents and carers at the school should be able to:

- Access & fully understand our age-appropriate Online-Safety & Acceptable Use Policies
- Use the internet appropriately & know their use can be monitored and traced to individual users
- Monitor children's social media use, especially if they are young or particularly vulnerable

Our students will be taught:

- to evaluate the content of online information e.g. whether representations of body image are photo-shopped or air-brushed
- To question who a person really is
- How other people portray their lives online
- How to spot fake news
- How to disengage and control their internet use

The school will:

- Take reasonable precautions to prevent student and staff access to inappropriate sites or material
- Maintain an audit of all ICT & social media use
- Teach pupils about responsible and safe use of the internet and what to do when things go wrong
- Ensure staff check sites and links before students use them
- Ensure all online platforms used to communicate with pupils and their families (e.g. learning online at home) are fully risk-assessed & monitored
- Ensure all staff and pupils are aware of and can access a clear reporting process for online-safety issues
- Ensure our Acceptable Use & Online-Safety Policies considers how all technology, online environments and mobile devices communicate, access social networks, music, videos and gaming sites, take photographs & record videos
- Carefully manage images and other identifying information about students, obtain full

consent before use, and delete images when a student leaves Meadowhead School.

It is a crime to:

- ***Harass or bully via text, email, or phone call***
- ***Create, possess, distribute indecent images ofchild even with consent or if self-generated***
- ***For an adult to have sexual communication with a child under 16 years***

The age of criminal responsibility is 10 years.

Online-safety Policy & Risk Assessment Appendix

Cyber-bullying can make children feel scared, upset, isolated & vulnerable, particularly as it can happen whilst alone and/or in their own home e.g.:

- Messages, texts, emails, photographs, video's, sexting, to individuals or groups
- Communicating threats, upset, offence, often with racist, sexist, or homophobic content
- Humiliating or abusive phone calls
- Inappropriate communication shared through social networking & gaming sites
- Encouraging other people to bully the victim
- Setting up fake profiles to make fun of someone
- Creating a false identity to send inappropriate communications in someone else's name
- Using chat rooms & gaming sites to threaten, abuse, lock out, &/or spread rumours
- Send viruses or hacking programs to harvest information or destroy someone's game/device
- Posting intimate, sensitive, personal information without someone's permission or knowledge

An adult may pretend to be someone online to befriend, obtain sensitive information or materials & threaten to expose information to the child's family or friends if they do not do as they say.

4 key concerns:

- **Content** – harmful material or ideas e.g. racist, pornographic, bullying, sexual, homophobic
- **Contact** – who interacting with online, are they encouraging student to do something harmful?
- **Conduct** – online behaviour e.g. making, sending, receiving explicit images, bullying, gambling
- **Commerce** – e.g. online gambling, inappropriate advertising, phishing, financial scams

Cybercrime is criminal activity using computers and/or the internet including:

- **Hacking:** unauthorised access to computers
- **Booting:** denial of Service (Dos or DDoS) attacks
- **Malicious software:** making/supplying/obtaining viruses, spyware, ransomware, botnets & Remote Access Trojans

If pupils have strayed into cyber-dependent crime – the DSL/D can refer them to Cyber Choices.

Youth gambling:

- 17% of under 16's gambled online in last 7 days
- Through adverts, apps, influencers, gaming
- Teach about gambling issues via the curriculum

Head Teachers & staff have powers to search pupils & their possessions, see:

- **'Reasonable force, searching & screening,Sept 21'** in education policies, procedures & guidance, on the Safeguarding Sheffield Children website.

Other issues:

- Taking a photograph without consent is an invasion of privacy & may be distressing
- Once photos are sent to a device, network, or website they are impossible to fully track or delete
- Giving out any personal information (including photos) could put someone at risk of harm
- Location tracking services allow any individual to identify the location of people & devices

Useful links:

- Safeguarding Sheffield Children website: Online Safety
- Sheffield Children Safeguarding Partnership Procedures - Online Safety
- UK Safer Internet Centre
- Screening, Searching & Confiscation: advice for schools, DfE 2018
- Safeguarding and remote education
- NSPCC NetAware
- Preventing Bullying, DfE
- NSPCC: Sexting
- Thinkuknow
- YGAM
- Sharing nudes and semi-nudes: advice for education settings working with children and young people, UKCIS, Dec 20

Risk-assessing unsafe internet use

- **Never publicise 'unsafe' sites** as it encourages people to look & implies other sites are 'safe'
- If child/parent/carer has already accessed a worrying site or there are other online-safety concerns, use the table below to assess their needs

Child or young person's level of need:

Universal	Universal plus/partnership plus	Targeted/acute/specialist
• Has a range of IT skillsand understands how the internet works and its global audience • Safely enjoys the benefits of the internet and can communicate safely with friends and family • Maintains personal security when using chat rooms, gaming etc. • Does not disclose personal details of friends to unknown parties • Family aware of use and understand safe use principles • Child shares interest with parents	• Some IT skills but doesn't really understand how the internet works • Uses the internet carelessly, visiting unregulated sites • Visits adult sites and views explicitly sexual or violent material • Is the victim or perpetrator of occasional low level cyber-bullying • Has IT skills but using them to access unsuitable areas of the internet • Uses the internet to establish contact with unknown others and discloses contact details • Transmits pictures/video of self or others which could be used by internet predator or for cyber bullying • Discloses address and phone details • Agrees to meet stranger with peer(s)	• Visits illegal sites or sites designed for adults and develops an interest which may lead to criminal or exploitative actions • Exposes friends to risk by disclosing details to strangers • Posts explicitly sexual/ violent material including photos/ video of self or others • Discloses stranger abuse resulting from internet contact • Is the victim or perpetrator of sustained and/or serious cyber-bullying that includes disclosure of personal and identifying information • Agrees to meet stranger alone

Action from practitioners:

• Child is benefiting from parental guidance and curriculum activity • Continue discussion about online safety in the curriculum	• Parents/carers & setting provide advice & consider next steps • Parents and carers are given advice as needed • Age appropriate access controls are put in place • Discuss with DSL/D in setting • Consider an action plan with parents/carers • Consider an FCAF to assess family needs	• Inform DSL/D immediately • Notify police • Inform parents/carers if safe to do so • If parents/carers may be part of the risk or if a crime may have been committed, **do not inform them before** you discuss with The Hub • **If a child/young person is at risk of significant harm refer them immediately to The Sheffield Safeguarding Hub, tel. 0114 2734855** • Notify other parents/carers if appropriate • Ensure other involved practitioners are aware of your concerns provide support