ONLINE SAFETY POLICY

MIDDLEWICH HIGH SCHOOL

Updated December 2022

Updated: December 2022
Approved by: Headteacher 04.12.2022
Review Date: December 2025

Document Control Information	
Document ID	MHSESAFETY01
Document title	MHS Online Safety Policy (previously e-safety policy)
Version	1.1
Status	APPROVED
Author	Sarah Colclough
Publication date	February 2020
Next review date	December 2025

Version History			
Version	**Date**	**Detail**	**Author**
1.0	February 2020	Initial	Steve Wiseman
1.1	December 2022	Updated	Sarah Colclough

Approvals	
Approver	**Date**
Governing Body	February 2020
Headteacher	04.12.2022

1. **Purpose**

Online Safety encompasses the use of new technologies, internet and electronic communications such as learning platforms, mobile phones, tablets, video conferencing, collaboration tools and personal publishing. It highlights the need to educate students about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

2. Aims

Our school aims to:

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

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')

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

2.1 This policy has links to other policies e.g. acceptable use, bullying, and safeguarding. The Senior Leader responsible for Safeguarding is Sarah Colclough.

3. Risks

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content (student as receiver) – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

Contact (adult-initiated activity) – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct (Student as actor)– personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and gambling, inappropriate advertising, phishing and/or financial scams

The school acknowledges its responsibility to foster informed discussion and protect students from the potential harm caused by extremist* attitudes of all sorts.

*The Government has defined extremism in the Prevent Strategy as "…vocal or active opposition to fundamental British Values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs."

4. Requirements on Users

3.1. All staff, students and parents/carers must read and sign the acceptable use contract (AUC) before using any of the school's ICT resource. (Please see Appendix 1)

3.2. The school has a central record of all staff and students who are granted ICT access. The record will be kept up-to-date, for instance a member of staff may leave or a student's access be withdrawn.

3.3. Students are not permitted under the AUC to use ICT equipment unsupervised.

3.4. Staff and students may only use the school's e-mail accounts on the school's system.

3.5. Mobile Phones can not be seen or used within the school between the hours of 8:30 and 15:10. The sending of abusive or inappropriate text messages is forbidden. Use of other personal devices for sound or image recording during formal school time is also prohibited.

3.6. Staff will not use non-school personal electronic accounts when contacting students but will use their school email account or, where telephone contact is required, will be issued with a school phone.

Features of the School System

4.1. Internet access is designed expressly for students and community use and includes filtering both at the remote IT support system and within the school appropriate to the age of the students.

4.2. The school ensures through the AUC that the use of internet derived materials by staff and students complies with copyright law.

4.3. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the remote IT support can accept liability for the material accessed, or any consequences of internet access.

4.4. The school will block/filter access to social networking sites, newsgroups and external email systems. Circumventing this, e.g. via proxy servers, is forbidden under the AUC and will result in disciplinary action being taken.

4.5. The school regularly audits ICT provision (in particular remote access logs and website tracking logs).

4.6. School ICT systems are reviewed regularly for capacity and security including virus protection.

4.7. Emerging technologies are examined for educational benefit and a risk assessment highlighting any necessary changes to this policy will be carried out before use in the school is allowed.

5. Keeping Users Informed

5.1. Students are taught about what internet use is acceptable and given clear objectives for internet use in both Computing and I- Media lessons

5.2. Online safety rules are posted in all rooms where computers may be used and discussed with the students at the start of each year.

5.3. All users are aware via the AUC that internet use is monitored and can be traced to the individual user.

5.4. All staff have access to this Online Safety Policy and its importance will be explained to new staff members.

5.5. Parents'/carers' attention will be drawn to the school's Online Safety Policy when their children join the school and again as appropriate e.g. in newsletters, the school website etc.

6. Privacy

6.1. Students must not reveal personal details of themselves or others which may reveal their identity or location in any electronic communication, or arrange to meet anyone without specific permission. They are advised to this effect when signing the AUC as well as in relevant lessons.

6.2. The only contact details on the school website will be the school address, e-mail and telephone number. Staff or students' personal information will not be published.

6.3. The Headteacher takes overall editorial responsibility for the website and ensures that content is accurate and appropriate.

6.4. Parents' and carers' consent for the publication of photographs of students and their work is obtained on joining the school and photographs of those who opt out are not used.

6.5. Students must not access or copy images used for learning within lessons at any other times.

6.6. Students' full names will not be used anywhere on any school system which is accessible to the public e.g. website, particularly in association with photographs.

6.7. The AUC insists that computers be locked when not in use to help prevent unauthorised access to personal data; the lock activates automatically after a set time.

6.8. Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation.

6.9. Staff who choose to access personal data e.g. student records from home do so in the knowledge that they are bound by this act and must use an encrypted device. Staff are not permitted to use removable storage devices.

7. Concerns

7.1. Students must immediately tell a teacher if they receive an inappropriate or offensive electronic communication including e-mail or text messages, including from their peers.

7.2. If students discover an unsuitable site it must be reported to a teacher and then via the support logging system to Novus who will block/filter the site or escalate as appropriate.

7.3. Complaints of internet misuse will be passed from the class teacher, to the Deputy Headteacher with responsibility for behaviour, attitudes and personal development.

7.4. Complaints about staff misuse will be referred to the Headteacher.

7.5. Complaints of a child protection nature must be dealt with in accordance with the school's safeguarding procedures.

7.6. If any student should approach a member of staff with an allegation involving inappropriate text messages or images of a sexual nature it is not appropriate for that member of staff to attempt to verify the nature of these texts or images by asking to look at them or agreeing to do so if a student or other party offers to show them. The correct response is to pursue the matter promptly with one of our Designated Safeguarding Professionals: Mrs Christmas, Mrs Colclough, Mrs Holt, Mrs Clarke Edwards, Mr Maxted, Miss Hinch or Miss Wilkinson. Those members of staff will follow Government Guidance and seek police advice as appropriate

Appendix 1: Acceptable use contract (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 or 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 usernames 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 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've 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 ● Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate ● 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 **I understand that the use of electronic devices and mobile phones are not permitted within school and if they are seen in school between the hours of 8:30 and 15:10, it will be taken to the** **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 Two (staff, governors, volunteers and visitors

Name of staff member/governor/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 who has consented to having their photograph taken.
- 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
- Leave my computer/ laptop/ electronic device open/ unlocked, whereby students can see/access information

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 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 Novus 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/governor/volunteer/visitor):

Date: