MONKSEATON HIGH SCHOOL
ONLINE SAFETY POLICY

Status:

Statutory policy or document	No
Review frequency	Annually
Approval by	Governing Body
Approval date	09.10.24

Publication:

Statutory requirement to publish on school website	No
Agreed to publish on school website	Yes

Review:

Frequency	**Next Review Due**
Annually	09.10.25

Version Control:

Author	**Creation / Revision date**	**Version**	**Status**
Business Manager (MAD)	11.10.23	1.0	Final approved version for publication.
Business Manager (MAD)	10.09.24	1.1	Minor formatting changes

1. Aims

At Monkseaton High School, we understand that information computer technology (ICT) is an essential resource for students, staff, governors and visitors. The internet, and other digital and information technologies, open up opportunities for students and play an important role in their everyday lives. ICT supports teaching and learning, pastoral and administrative functions of the school. We understand the need for safe and appropriate use as ICT resources and facilities also pose a risk to data protection, online safety and safeguarding.

We aim to:

- Set guidelines and rules on the use of school ICT resources.
- 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.
- Support in students learning about safe and effective internet and ICT use.

The 4 key categories of risk

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

1. Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, homophobia, self-harm, suicide, antisemitism, radicalisation and extremism.
2. Contact – 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.
3. Conduct – 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.
4. Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

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 schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-

bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' 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 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All Governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2).
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's Designated Safeguarding Lead (DSL) and deputies (DDSL) are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher, Business Manager, ICT Technician and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the Safeguarding and Child Protection Policy.
- Ensuring that any online safety incidents are logged (see appendix 3) 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 the Behaviour Policy.
- Updating and delivering staff training on online safety.

- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the Headteacher and/or Governing Body.

This list is not intended to be exhaustive.

3.4 The ICT Technician

Under the guidance of the Business Manager, the ICT Technician is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT 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 school's ICT systems on a monthly basis.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Provide regular reports on keywords searched and websites blocked analysing for patterns / trends.
- Ensuring that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy.
- Ensuring 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.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2) and ensuring that students follow the school's terms on acceptable use (appendix 1).
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 3) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms of acceptable use (appendix 2).

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum: The text below is taken from the National Curriculum computing programmes of study. It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All secondary schools have to teach relationships and sex education and health education.

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.

By the end of secondary school, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online.
- The impact of viewing harmful content.
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail.
- How information and data is generated, collected, shared and used online.
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours.
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online).

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

5. Educating parents about online safety

We will raise parents' and carers' awareness of internet safety in letters or other communications home, and in information on our website. This policy will also be shared with parents via our website.

We will let parents know:

- What systems the school uses to filter and monitor online use.
- What students are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online.

If parents / carers 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.

6. Cyber-bullying

6.1 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. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We 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.

We will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form tutors will discuss cyber-bullying with their tutor groups.

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, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, 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 students, we will use all reasonable endeavours to ensure the incident is

contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher (as set out in the behaviour policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the Headteacher / DSL or a Deputy DSL.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.
- Seek the student's cooperation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent refuses to delete the material themselves.

If a staff member suspects a device may contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- Not view the image.
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.

Any searching of student's will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.
- Our behaviour policy.

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

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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

More information is set out in the ICT and internet acceptable use policy and the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Students may bring mobile devices into school, but are only permitted to use them outside or on the ground floor during break and lunch time. At all other times they must be turned off and stored within student's bags. 6th Form students may also use mobile devices in the 6th form area.

Any breach of the acceptable use agreement by a student will trigger a sanction in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using work devices outside school

We will take appropriate steps to ensure that devices remain secure when used away from the school premises. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).

- Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.

If staff have any concerns over the security of their device, they must seek advice from the ICT Technician.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

10. How the school will respond to issues of misuse

Where a student 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. 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.

11. 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).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages.
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
    - Sharing of abusive images and pornography, to those who don't want to receive such content.
    - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and 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.

Governors 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 3.

This policy will be reviewed every year by the Business Manager. At every review, the policy will be shared with the Governing Body.

13. 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.
- Staff code of conduct.

Appendix 1: Student Acceptable Use Agreement.

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS
Name of student:
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 member of staff is present, or with a member of staff'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 a member of staff or my parent/carer. • Tell a member of staff 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 a member of staff 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 member of staff. • 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. 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 permission from a member of staff. • 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: **Date:**

*paper forms will be replaced by with Microsoft forms and electronic signatures.

Appendix 2: Staff / Governors / Volunteers / Visitors Acceptable Use Agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF / GOVERNORS / VOLUNTEERS / VISITORS
Name of staff / 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 students without proper reason and without consent. • Share confidential information about the school, its students 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 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 Technician know if a student 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 students in my care do so too.
Signed: **Date:**

*paper forms will be replaced by with Microsoft forms and electronic signatures.

Appendix 3: 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**

Equality Impact Assessment

1. Name of the change, strategy, project or policy:	ICT & E safety Policy
2. Name of person(s) completing this form:	Marie-Anne Dowson

3. Has the policy/practice been assessed to consider any potential impact on the equality groups? Yes

Where potential impact has been identified, please complete questions 5-9, if none is identified, please sign and proceed to question 10.

4. Equality Target Group (highlight):	**Negative impact – it could disadvantage**	**Reason**
Race **Religion/belief** **Disability** **Gender** **Gender Reassignment** **Sexual Orientation** **Age** **Pregnancy/Maternity** **Marriage & Civil Partnerships**	**No significant impact.**	

5.	**Yes**	**No**
Is the impact legal/lawful? Seek advice from your School link HR Advisor if necessary.		
Is the impact intended?		
Does this action/policy/procedure attempt to meet the aims of the public sector equality duty? (this should feed into your Single equality scheme & action plan)	Yes, No, or N/A	If yes, please provide details
Eliminate unlawful discrimination, harassment and victimisation		
Advance equality of opportunity between different equality groups		
Foster good relations between different equality groups		

7. If you have identified any negative impact, have you identified any ways of avoiding or minimising it?

8. Is it possible to consider a different policy/strategy/action, which still achieves your aim, but avoids any negative impact on people?

9. In light of all the information detailed in this form; what practical actions would you take to reduce or remove any negative impact?

10.a) As a result of the assessment and consultation completed in Part A above, state whether there will need to be any changes made to the policy, project or planned action.

10.b) As a result of this assessment and consultation, does the school need to commission specific research on this issue or carry out monitoring/data collection?

A) No changes required.

11. Have you set up a monitoring/evaluation/review process to check the successful implementation of the policy, project or change? If yes please provide details below.	**Yes**			

Bi-annual review and report to governing body.