

ONLINE SAFETY POLICY

2023



Approved by:	Full Governance Board
Date approved:	Spring Term 2023
Next review:	Spring Term 2024
Policy owner:	Acting Vice Principal – Safeguarding

Contents

1. Aims	3
2. Legislation and guidance	3
3. Roles and responsibilities	4
4. Educating students about online safety	6
5. Educating parents about online safety	7
6. Cyber-bullying	7
7. Acceptable use of the internet in school	8
8. Students using mobile devices in school	8
9. Staff using work devices outside school	9
10. How the school will respond to issues of misuse	9
11. Training	9
12. Monitoring arrangements	10
13. Links with other policies	10
Appendix 1: KS3, KS4 and KS5 acceptable use agreement (students and parents/carers)	10

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and Trustees
- 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

The 4 key categories of risk

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

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism and all other forms of hate speech
- **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
- **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; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

2.1 Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 Principals 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 students' 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.

This policy complies with our funding agreement and articles of association.

2.2 GDPR

- From time to time data may be collected by the school via online forms, website or e-mail, e.g. for questionnaires, questions given for homework. If data is collected in this way, it will be kept in accordance with current Data Protection Act legislation / GDPR.
- Data will be held on secure servers outside the UK. By signing this document and/or the Home School Agreement, parents are consenting to the use of this service.

- The North Halifax Grammar School website <http://www.nhgs.co.uk> provides information for members of the public. The aim of the website is to provide information to such groups about our activities and to support teaching, as well as to promote the work that goes on in school (this may include students' work, photographs, sound and video). Images of students on the school website help to promote the positive work that happens in the school and helps to motivate students involved. There is a risk that images may be downloaded and used for inappropriate means. To avoid this, the school takes into account the following statement when considering whether photographs and moving images of students should be included on the school's website:

A photograph of an individual (which is not considered a group photograph) will not normally be used. However, if such a photograph is needed, then the school will require that a separate permission form to be completed. In the event that a photograph does appear on the website in error, please inform the school at the earliest opportunity in order to get it removed. A group photograph is considered to be at least 3 students. If a group photograph is shown, first names may be given but not necessarily in the order that the students are shown. Students, who appear in photographs, must be in suitable dress and in a non-compromising pose in order to reduce the risk of inappropriate use.

- By signing the school's consent form, you are agreeing to allow group photographs of your son/daughter being published on our website. If you do not wish for photographs of your son/daughter to be included on the website, then please inform the school in writing.

3. Roles and responsibilities

3.1 The Trustees

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

The Trustees 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).

The Trustee who oversees online safety is Amanda Cade.

All Trustees 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, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with SEND 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 DSL deputies 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, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged 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 school 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 Trustees

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager 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
- Ensuring that any online safety incidents are logged 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 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'
- Staff should not store photographs on their own devices. If a photograph is taken at an event, this should be forwarded to the Marketing Officer and then deleted from the device. Staff should not put photographs of students on their own social media sites.
- Should any member of staff come across a website which has illegal content they must report it using the appropriate procedures and to the Internet Watch Foundation <http://www.iwf.org.uk>

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

If a student brings their own device into school, parents must ensure they have the necessary insurance to cover the device against any accidental damage or theft. Students should access the internet via the school's wifi which provides filtered access. Should the student access the Internet via their mobile network provider's network (e.g. 3G / 4G network) then the school does not have any way to control or filter any content that is delivered or sent to or via the device. Parents have the responsibility to provide adequate filtering and parental controls for such devices, for instances when students are not connected to the school's network.

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 resource sheet – [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)

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 on 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 schools have to teach:

- [Relationships education and health education](#) in primary schools
- [Relationships and sex education and health education](#) in secondary schools

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

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

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.

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 anti-bullying 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. The school will actively discuss cyber-bullying with students, 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.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Religious, Personal, Social and Economic (RPSE) education, and other subjects where appropriate.

All staff, Trustees 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 for Learning policy. Where illegal, inappropriate or harmful material has been spread among students, 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.

If a student is being bullied via electronic methods then if possible, follow the guidelines below;

- Do not respond to the communication under any circumstances
- If possible, save the message as this can be used as evidence at a later date. Don't delete it.
- Speak to a teacher / friend / parent / carer

- Block the sender/s of the email by using the 'Junk Email' or 'Spam Filter' provided by the web mail account provider
- Report via the 'Report-IT' online form, available via the School website. (<http://www.nhgs.co.uk/reportit>) or inform a member of staff

Students can find out more about cyber bullying on the Childline (www.childline.org.uk) website or contact them by telephone on 0800 1111.

Students should familiarise themselves with the content on the 'Think You Know' website (<http://www.thinkuknow.co.uk>) operated by The Child Exploitation and Online Protection Centre (CEOP). Students should exercise caution over whom they give their contact information to, such as email addresses and telephone numbers etc.

6.3 Examining electronic 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 students' 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 believed to be on the device, staff should not view it. The phone should be given to the DSL who will decide what action should be taken.

Any searching of students will be carried out in line with:

- The DfE's latest guidance on [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- The school's COVID-19 risk assessment

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 Trustees 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.

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

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

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

8. Students using mobile devices in school

Students may bring mobile devices into school, but are not permitted to use them during:

- Lessons, unless permission is given by the member of staff, or whilst moving around the school.

Any use of mobile devices in school by students must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device, and / or other appropriate sanctions.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. 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 their 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 – always install the latest updates

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.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from their Line Manager and / or the IT Manager.

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 Behaviour for Learning policy. 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 or other forms of hate speech
 - 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 the risks up

- 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.

Trustees 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 using CPOMS.

This policy will be reviewed every year by the Vice Principal i/c Safeguarding. At every review, the policy will be shared with the Trustees. The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour for Learning policy
- Disciplinary policy
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy (staff and students)
- Risk Register
- Anti-bullying policy

Appendix 1: KS3, KS4 and KS5 acceptable use agreement (students and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS

Name of student:

I will read and follow the rules in the Online Safety 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
- Keep my username and passwords safe and not share these with others
- Keep my private information safe at all times and seek advice before giving my name, address or telephone number to anyone online
- Tell a responsible adult immediately if I find any material which might upset, distress or harm me or others
- Keep my device in a secure place and if my device is lost, stolen or sold, I will inform school
- Have phone locking software installed should my phone get lost/stolen
- Use my own personal Google account when setting up my own Android device, not school's.
- Carefully consider the origin of an email before opening any attachments or following any links. If I have concerns regarding an email I will not open it and will forward it to 'stop@nhgs.co.uk') so it can be investigated further) then delete it.
- Always use my own account and 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
- Attempt to gain unauthorised access to files, emails or settings
- Attempt to by-pass the school filtering or firewall or try to access content which is banned
- Set up websites or groups using the school's name, initials or logo, or anything else which clearly identifies the school, without permission.
- Store or run software or files which are unauthorised
- Contact teachers via my own personal e-mail, I will always use my school e-mail
- Plug my own laptop or device directly into network ports, I will use the school wifi
- Take pictures of students or staff in school without following the guidelines within the Acceptable Use policy
- 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/carers, 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 without a member of staff 's permission or whilst moving around the school
- I will connect to the school wifi to access the internet
- 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 (student):

Date:

Parent/carers' 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 students 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/carers):

Date:

Appendix 2: acceptable use agreement (staff, Trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS AND VISITORS – THIS SHOULD BE READ ALONGSIDE THE STAFF CODE OF CONDUCT WITHIN THE STAFF HANDBOOK

Name of staff member/Trustee/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 other than for professional purposes
- Use any improper language or content 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 checking the guidance in this policy first
- Share confidential information about the school, its students or staff, or other members of the community
- Access, modify or share data without proper authorisation
- Use school facilities to pursue personal business interests, for gambling or for political purposes not directly related to your job

- 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 and will use my work email for school business
- 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 and keep all data securely stored in accordance with this policy and the school's data protection policy. I will set up and use two factor authentication for email.
- When planning lessons, I will ensure that any websites used do not contain any inappropriate or misleading material
- I will let the designated safeguarding lead (DSL) and ICT manager 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.
- I will carefully consider the origin of an email before opening any attachments or following any links. If I have concerns regarding an email I will not open it and will forward it to 'stop@nhgs.co.uk' (so it can be investigated further) then delete it
- I will ensure that I log out of the system or at least lock my account whenever I leave a computer and will take care to ensure information, such as email and login details are not displayed on the whiteboard in lessons. P

Signed (staff member/Trustee/volunteer/visitor):

Date: