Hadrian Learning Trust

Online safety policy

Reviewed: September 2023

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils/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 with and address 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, antisemitism, radicalisation and extremism

- **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 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

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 – remove if not applicable, see section 4]
- Searching, screening and confiscation
- Filtering and Monitoring

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'/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 Hadrian Learning Trust's funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Trust Board

The Trust Board has overall responsibility for monitoring this policy and holding the executive headteacher to account for its implementation.

The Trust Board will, through the designated safeguarding trustee, make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The Trust Board will also make sure through the designated safeguarding trustee that all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The Trust Board will, through the designated safeguarding trustee, meet with appropriate staff to discuss online safety, requirements for training, and monitor online safety issues as provided by the online safety lead and designated safeguarding leads (DSLs).

The Trust Board will ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Trust Board must ensure the schools have appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The Board, through the designated safeguarding trustee and the executive headteacher, will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting these standards, which include:

- identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- reviewing filtering and monitoring provisions at least annually;
- blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- having effective monitoring strategies in place that meet safeguarding needs.

All trustees will:

- Ensure that they have read and understood this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure, through the designated safeguarding trustee, that online safety is a running and interrelated theme while devising and implementing their trust and school approaches to safeguarding and related policies and/or procedures
- Ensure through the designated safeguarding trustee that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils/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 Executive Headteacher

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

3.3 The Designated Safeguarding Leads and Online Safety Lead

Details of the Trust's Designated Safeguarding Leads (DSLs), and deputy DSLs and Online Safety Lead are set out in Hadrian Learning Trust's child protection and safeguarding policy as well as in relevant job descriptions.

The DSL in each school takes lead responsibility for safeguarding in school, with support from deputy DSLs and the Online Safety Lead. The Online Safety Lead is responsible for:

- Supporting the executive headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

- Working with the executive headteacher and Trust Board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the executive 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's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) 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 (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the executive headteacher and/or trust board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular online safety updates to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The Network 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 pupils/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
- 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

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including agency staff, and contractors and volunteers with access to the schools' IT systems or internet 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 pupils/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 and anti-bullying policies
- Responding appropriately to all reports and concerns about sexual violence and/or harassment and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Ensure that they and their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)
- Notify the school if any concerns or queries about online safety

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
- Parent Courses - National Online Safety

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 be expected to read and follow it. Where relevant, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils/students about online safety

Pupils/students will be taught about online safety as part of each school's stay safe and well curriculum.

5. Educating parents/carers about online safety

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

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 and anti-bullying policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils/students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils/students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The schools will actively discuss cyber-bullying with pupils/students, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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, trustees and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils/students, as part of safeguarding training (see section 11 for more detail).

The schools also send 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 schools will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils/students, the schools will use all reasonable endeavours to ensure the incident is contained.

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

6.3 Examining electronic devices

The executive headteacher, and any member of staff authorised to do so by the executive headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting it:

- Poses a risk to staff or pupils/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

Searches will be carried out in accordance with our carry our Screening, Searches and Confiscations Policy.

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 been 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 / executive headteacher / lead for online safety 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 pupil/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 pupils/students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation, which informs Hadrian Learning Trust's policy
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

7. Acceptable use of the internet in school

All pupils/students, parents, staff, agency staff 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 purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils/students, staff, volunteers, trustees and visitors to ensure they comply with the above.

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

8. Pupils/students using mobile devices in school

Pupils/students may bring mobile devices into school but are not permitted to use them during the school day unless given express permission by the member of staff responsible for them at the time.

Any use of mobile devices in school by pupils must be for educational purposes and in line with the acceptable use agreement (see appendices 1 and 2).

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

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 files are not stored on the device. Files should be stored on the appropriate server (school server or Microsoft 365)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends

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, or code of conduct.

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 the Network Manager.

10. How the school will respond to issues of misuse

Where a pupil/student misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour 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 disciplinary policy. 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 other children 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 pupils/students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils/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. The lead for online safety will undertake online safety training 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. Filtering and Monitoring

The Trust exercises its right to monitor, by electronic means, the use of each school's computer systems, including key logging, the monitoring of web-sites, the interception of e-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

The Trust meets the standards set out for digital technologies in school updated in March 2023:

- The trust has identified and assigned roles and responsibilities to manage filtering and monitoring systems (see 3. Roles and Responsibilities)
- An online safety review takes place annually and includes reviews of filtering and monitoring

- The filtering systems block harmful and inappropriate content, without unreasonably impacting teaching and learning. These systems have been checked against the UK Safer Internet Centres guidance on appropriate filtering, and are tested regularly to ensure they block content as outlined in KCSIE

13. Cyber Security

The Trust take responsibility for ensuring an appropriate level of protection procedures is in place in order to safeguard the systems, staff, learners. Online Safety reviews take place annually in order to review the effectiveness of these procedures to keep up with evolving cyber-crime technologies.

The Trust works with various organisations including other schools, service providers, the North East Regional Cyber Crime Unit and the North East Business Resilience Centre to educate staff, students and trustees, and develop policies and procedures.

14. Monitoring arrangements

The DSLs log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Safeguarding Group. At every review, the policy will be shared with the trust board. The review will be supported by an annual assessment of risks that considers and reflects the risks pupils/students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff code of conduct
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use agreement

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

Name of pupil/student:

I will read and follow the rules in this Acceptable Use Agreement.

When I use the school's ICT systems (e.g. computers) and access 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, telephone number or email address to anyone online without the permission of my teacher or parent/carer
- Tell a teacher (or responsible adult) immediately if I find any material which might upset, distress or harm me or others
- Always log off 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
- Access, 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
- Eat or drink in computer rooms
- Attempt to fix or move equipment or peripherals myself

If I bring a personal mobile phone or other personal electronic device into school:

- I will not use it during the school day without a teacher's permission
- If given permission, 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 my use of the school's ICT facilities and systems.

I understand that there will be consequences if I do not follow the rules.

Signed (pupil/student):	**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 my child 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:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, TRUSTEES, VOLUNTEERS AND VISITORS

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 on to the school's network using someone else's details
- Take or store photographs of pupils/students on personal devices
- Share confidential information about the schools, the pupils/students or the staff, or other members of the schools' communities
- Access, modify or share data that I am not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school and you have the permission of the Executive Headteacher

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
- 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
- Ensure that any personal online content does not bring the Trust into disrepute or breach my obligation to professional standards. I will ensure that privacy and security settings are enabled on social networking sites, including the prevention of messages being sent as a result of searches. I will not access social networking platforms on school equipment, or while directly responsible for pupils/students
- Inform the designated safeguarding lead (DSL) and network manager 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
- Always use the school's ICT systems and internet responsibly, and ensure that pupils/students in my care do so too

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

Signed (staff member/trustee/volunteer/visitor):	**Date:**