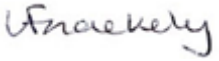
Hawkley Hall High School

POLICY NAME: Online Safety

ADOPTED: November 2023

REVIEW PERIOD: November 2024

SIGNATURE: 

Chair of Governors

The Rowan Learning Trust

Aims

Hawkley Hall High school aims to:

- have robust processes in place to ensure the online safety of students, 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.

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.
- *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;
- *Commerce* – risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

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 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 learners' electronic devices where they believe there is a 'good reason' to do so.

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

Roles and Responsibilities

Governors

The local governing body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation. They 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.
- 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 learners 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.

The headteacher

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

The leadership team

The leadership team 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.
- working with the DSL/DDSL, 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 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 committee.
- The DSL and other key stage monitor Impero for inappropriate use of ICT/searches

Details of our DSL and DDSLs are set out in our Safeguarding Policy.

The Trust ICT manager

The Trust 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.

Together with our ICT technician:

- conducting a full security check and monitoring the school's ICT systems regularly on a proactive basis and reactively as needs/situations arise.
- blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

All staff and volunteers

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

- reading and 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.
- ensuring that students follow the school's terms on acceptable use;
- working with the DSL/SLT 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 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'.

Parents and carers

Parents and carers are expected to:

- notify a member of staff or the headteacher of any concerns or queries regarding this policy.

Parents and carers 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

Visitors and members of the community

Visitors and members of the community who use our ICT systems or internet will be made aware of this policy, when relevant, and are expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating students about online safety

All schools have to teach:

- Relationships and sex education and health education

We recognise that our students have had a disrupted educational experience and will therefore have considerable gaps in their knowledge and skills. Some of our students are also vulnerable and therefore it is even more important that we address their individual learning needs.

We ensure our students know:

- understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- report a range of concerns.

- 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 learners with SEND.

Students will be taught about online safety as part of the curriculum.

Educating parents/carers about online safety

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

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with their child's Head of Year.

Concerns or queries about this policy can be raised with any member of staff.

Cyber-bullying

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.

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 actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. Staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying, including personal, social, health and economic (PSHE) education, and other subjects where appropriate.

In relation to a specific incident of cyber-bullying, we follow the processes set out in our Anti-Bullying Policy. Where illegal, inappropriate or harmful material has been spread among learners, the school 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 grounds to suspect possessing that material is illegal. They will work with external services if it is deemed necessary to do so

Examining electronic devices

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

- poses a risk to staff or learners, 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, or their deputy.
- 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 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 member of staff in conjunction with the DSL and the headteacher or their deputy 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 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 (or equivalent) 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 students 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

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through our complaint's procedure

Reporting Concerns

All staff record any concern about or disclosure by a pupil of abuse or neglect and report this to the D/DSL using CPOMS

(or a concerns form if you do not have access to a computer.) It is the responsibility of each adult in the school to ensure that the D/DSL receives the record of concern without delay.

All staff should be aware that children may not feel ready or know how to tell someone that they are being abused, exploited, or neglected, and/or they may not recognise their experiences as harmful.

.

Acceptable use of the internet in school

Visitors are expected to read and agree to our terms on acceptable use if relevant.

Use of our 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 students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

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 in line with the Trust's policy.
- 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.
- ensuring 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.
- keeping operating systems up to date by bringing the device into school at least once each half term and connecting to the network so that routine updates can be installed.

Staff members must not use the device in any way which would violate the school's terms of acceptable use.

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 ICT team.

How the school will respond to issues of misuse

Where a student misuses our ICT systems or internet, we will follow the procedures set out in our policies. 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 our ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be discussed with the Trust's Director of HR and then dealt with in accordance with recommendations and relevant Trust/school 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

Training

As part of their induction new staff receive training on online safety, Safeguarding and Prevent training.

All staff receive refresher training at least once a year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

All staff are 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 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

The DSL and DDSL undertake child protection and safeguarding training, which includes online safety, at least every 2 years. They also update their knowledge and skills about online safety at regular intervals, and at least annually.

Governors

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers

Volunteers will receive appropriate training and updates, if applicable.

Monitoring arrangements

Staff log behaviour and safeguarding issues related to online safety using Class Charts. This policy will be reviewed annually. At every review, the policy will be shared with the governing body.