



ROOKS HEATH SCHOOL
Strive to be your best

ONLINE SAFETY POLICY

Term of policy: Annual

Approved by: LGB 24.6.26

Date ratified: BoT 7.7.26

Next Review Date: Summer 2027

Author: L Hyde

Sources: The Key

Online Location: SharePoint / Staff / Policies

Consulted with JCC? Yes No

Introduction

This policy replaces any previous policy and follows the DfE regulations.

As part of our commitment to meet the Public Sector Equality Duty (PSED) requirement, to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations. We have carefully considered the impact of this policy on equality. The school will ensure that this policy is applied fairly to all employees and does not have a negative impact on students or staff with protected characteristics, race, sex, religion and belief, sexual orientation, age, disability, gender reassignment, marriage and civil partnership and pregnancy and maternity.

1. Aims

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

2. 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 (RSE)
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation and filtering and monitoring standards.

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 PSHE and Computing programmes of study.

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

All online safety practices will align with UK GDPR and the Data Protection Act 2018, ensuring:

- Personal data is handled securely.
- Staff understand data sharing risks online.

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). There is a governor who oversees online safety.

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 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 DSL and children safeguarding team 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, AHT Digital Lead, Network Manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy. The DSL will escalate serious incidents to the Headteacher and external agencies (e.g. police, social care) where required. The Headteacher will involve the Local Authority Designated Officer (LADO) where staff conduct is concerned.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Carry out regular online safety risk assessments with the AHT Digital Lead, considering:
 - Emerging technologies and platforms
 - School specific risks (e.g. local issues, student demographics)
 - Effectiveness of existing controls
 - Updating and delivering staff training on online safety
 - Liaising with other agencies and/or external services if necessary
- Checking filtering and monitoring reports provided by the Network Manager and/or filtering and monitoring provider.
- Responding to safeguarding concerns identified by filtering and monitoring.
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly.
- Providing regular reports on online safety, in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Network Manager

The Network Manager is responsible for:

- Implementing and maintaining appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Providing filtering and monitoring reports to the DSL and AHT Digital Lead
- Completing actions following concerns or safety checks.
- 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 daily basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are reported to the DSL and AHT Digital Lead, logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are reported to the DSL and AHT Digital Lead, logged and dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 The SLT Digital Lead

The SLT Digital Lead is responsible for:

- Buying filtering and monitoring systems
- Documenting decisions on what is blocked or allowed and why
- Reviewing the effectiveness of the schools filtering and monitoring provision
- Overseeing filtering and monitoring reports
- Ensuring that staff:
 - understand their role in regard to monitoring and filtering
 - Are appropriately trained in monitoring and filtering
 - Follow policies, processes and procedures in regard to monitoring and filtering
 - Act on reports and concerns
- Reviewing filtering and monitoring systems regularly to ensure they are effective, proportionate and appropriate to the school's safeguarding needs.

3.6 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 3), and ensuring that students follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Reporting safeguarding concerns immediately and no later than the end of the working day.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Maintain professional boundaries online at all times
- Not communicate with students via personal accounts
- Ensure social media use does not bring the school into disrepute

This list is not intended to be exhaustive.

3.7 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.

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 factsheet - [Childnet International](#)

3.8 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.

4. Educating students about online safety

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

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

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

The school will gather student voice on online safety through surveys, student council and discussion groups to inform policy and teaching.

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.

There will be parental contact events, in which a section is dedicated to communicating with parents about their child's responsible use of social media and digital technology. Additionally, an online safety evening is offered to parents. All parents are encouraged to attend.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children 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 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.

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. 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, 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.

6.3 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 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 DHT Pastoral.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil'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 / DHT Pastoral 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 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](#)
- Our behaviour policy / Searching, Confiscation and Screening protocol

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

8. Personal Devices / BYOD (Bring Your Own Device)

Students are not to use smart phones and mobile phones (or similar mobile devices that can access the internet, record and transmit text, sound, images etc.) on the school site, other than to set up the Microsoft Authenticator app and the Bromcom Student Portal with prior arrangement, under the direct supervision of appropriate staff. For details about the management of student mobile phones on site, please see the Mobile Phone policy.

The use of personal devices to access school systems or networks must comply with security requirements, including:

- Secure passwords
- Up-to-date software
- Use only approved platforms

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) and follow current NCSC guidance, for example using three random words.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Keeping operating systems, anti-virus and anti-spyware software up to date by always accepting the latest update and regularly restarting the device.
- Reporting any loss or damage to ICT Support without delay.

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 Network Manager.

10. Artificial Intelligence (AI) & Emerging Technologies

The school recognises the increasing use of artificial intelligence (AI) tools. Staff and students will adhere to the Use of AI policies and:

- Use AI responsibly and ethically.
- Not rely on AI to generate harmful, misleading or inappropriate content.
- Be aware of data privacy risks when using AI platforms
- Not input personal or sensitive data into AI tools unless approved.

11. Remote Learning/ Online Platforms

When learning takes place online or remotely:

- Only approved platforms (e.g. Microsoft Teams) will be used.
- Communication between staff and students must remain professional and take place within school systems.
- Sessions may be recorded where appropriate for safeguarding purposes.

12. 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 Code of Conduct and Disciplinary Procedures Relating to Misconduct. 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.

13. Training

All new staff members will receive training (Professional Development – PD), 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).

The DSL and children safeguarding team 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.

14. Monitoring arrangements

The DSL and members of the safeguarding team report safeguarding incidents related to online safety on the safeguarding software (MyConcern).

Online safety logs will be reviewed regularly to identify patterns, trends and emerging risks, informing future safeguarding actions.

Online safety incidents are included as reporting safeguarding to the board of governors.

This policy will be reviewed every year by the Assistant Headteacher – Digital Technology & Innovation. At every review, the policy will be shared with the governing board.

15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour for learning policy
- HR Policies Suite
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable use of ICT Policy
- Social Media Policy
- Searching, Confiscation & Screening Protocol
- Mobile Phone Policy
- Use of Artificial Intelligence Policies
-

These documents can be found on the Rooks Heath School website and SharePoint > Staff > Policies.