Online Safety Policy

January 2026

THE JO RICHARDSON

SUCCESS FOR ALL

COMMUNITY SCHOOL

ACHIEVE

Date of previous review	November 2023
Review frequency	Every two years
Date of next review	January 2028

Contents

Designated Safeguarding Lead: Amy Howe

Head of Computing and ICT: - Michael Campbell

ICT Network and Systems Manager: - Daniel Trayler

As a school we understand that social media and the online world can be all consuming for a stakeholder. We have been a mobile free school for over a decade. This is because we want our students to have a rest from the intense online world while they are in school. The following policy has been written with the intention of showing the controls and measures we have in place to both protect stakeholders and to also capitalise on the benefits the online world offers.

1. Aims

Jo Richardson Community 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
- Use social media to offer support and guidance to stakeholders who may need it in times of crisis

The four 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 (eg, 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
- 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 also considers the requirements of DfE guidance around the digital and technology standards in schools. More information about this can be found using the link below

https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-standards-for-schools-and-colleges#:~:text=An%20effective%20filtering%20system%20needs,assess%20and%20manage%20risk%20themselves

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). The Governor who oversees online safety is Eugene Dwaah (Safeguarding Governor).

The Governing Body will 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. All staff will complete the Hays online training on an annual basis.

The Governing Body will also make sure 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. Daniel Trayler (Network Manager) will provide information to the Governors to ensure they can execute this duty.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL). The ICT Manager will oversee this and provide the requirement information.

The Governing Body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Governing Body must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with the ICT Manager and service providers what needs to be done to support the school in meeting those 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 their safeguarding needs.

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 or college 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 (DSL)

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 Safeguarding and Child Protection Policy;
- Ensuring that any online safety incidents are recorded 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 Management Policy;
- Updating and delivering staff training on online safety;
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the Headteacher and/or Governing Body;
- Undertaking annual risk assessments that consider and reflect the risks children face;

- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively;
- Monitor the use of social media (please also see the Social Media Policy).

This list is not intended to be exhaustive.

3.4 The ICT Network and Systems Manager

The ICT Network and Systems 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 weekly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring that any online safety incidents are recorded 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 Management Policy;
- Overseeing the filtering and monitoring systems used in the school.

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 and ensuring that students follow the school's terms on acceptable use;
- Working with the DSL to ensure that any online safety incidents are recorded 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 Management Policy;
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

3.6 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;
- Monitor their child's use of online platforms and social media;
- Alerts the school in a timely fashion if there is anything that could put their child at risk;

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 resources – https://nationalonlinesafety.com/
- Reporting online abuse to the police – CEOP

National College – https://nationalcollege.com/categories/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 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.

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 (eg, 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.

Online safety will also be covered during Progress Evenings and via the school newsletter. We promote the National College safety group #wakeupwednesday.

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. The school is a member of the National Online Safety organisation which provides whole school community training, resources and parent guides to effectively safeguard students online. We encourage parents and students to download the app and visit the website. https://nationalcollege.com/categories/online-safety

6. Cyber-bullying

We are very clear that this is a mobile free school. If parents choose to get their child a phone, then we ask them to take responsibility for it. This includes monitoring its use, ensuring the appropriate filters are in place and that regular checks occur. There is nothing worse than thinking of a child being bullied in their own home due to open social media content.

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 Management 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 and Heads of Year will discuss cyber-bullying with their tutor groups.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. 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 Management 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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Students will also be educated about their responsibilities online. Staff will always act if they are provided with information about inappropriate use.

6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher (as specified in our Behaviour Management Policy and our Searching, Screening and Confiscation Policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

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

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff;

- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it;
- Seek the student's cooperation.

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

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

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

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

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

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

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

- **Not** view the image;
- Confiscate the device and report the incident to the DSL (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: https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-peoplenudes: 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 Management Policy / Searching, Screening and Confiscation Policy.

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

The Schools Police Liaison Team will be informed about any causes for concern and may be called to assist with any investigation as appropriate.

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. We recognise that AI has many uses to help students learn but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

We will treat any use of AI to bully students in line with our Behaviour Management Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used. This is especially the case when marking work and other submitted work.

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. Students using mobile devices in school

The school is a mobile free zone. This means students must not use their phones in the building at any point in the day. Staff are permitted to use their phone in their personal offices or the staff room. This policy is in place to safeguard all stakeholders. This includes clubs before or after school, or any other activities organised by the school. Any use of mobile devices in school by students must be in line with the Acceptable Use Policy.

Any breach of the Acceptable Use Policy by a student may trigger disciplinary action in line with the school Behaviour Management 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 (eg, 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 by always installing the latest updates.

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 manager.

Staff must not use their personal devices (including mobile phones) to communicate with students under the age of 18. This is even if they have left school.

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems, 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 and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

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

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

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

Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.
Training will also help staff:

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

The DSL will undertake child protection and safeguarding training, which will include online safety, at least every two 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 Safeguarding and Child Pprotection Policy.

12. Monitoring arrangements

The school currently have the following online safety solutions in place:

- Impero Education Pro;
- Webscreen filtering;
- HomeProtect;
- Sophos Endpoint Protection;
- R;pple Browser Extension.

Impero Education Pro
Software client installed on all school owned devices providing ICT Support staff with real-time monitoring, keyword detection and capture management.

Impero supplies a managed keyword policy providing appropriate monitoring compliance with KCSiI and UK Safer Internet Centre.

When keywords are triggered, a screenshot is taken of the device (including logged in user, date and timestamp) which is then sent to ICT Support via email for review.

Webscreen filtering
Internet filter provided/managed by our Internet Service Provider (ISP) LGfL (London Grid for Learning). Webscreen is hosted by LGfL so all incoming/outgoing traffic is subject to the filter and firewall.

ICT Support staff have access to block and/or allow websites and have the ability to run reports on activity through the filter system.

HomeProtect
Software client (provided by our ISP) that enforces the same web filtering on school owned devices that are loaned out to staff and students.

Sophos Endpoint Protection
AntiVirus software that is installed on all school owned devices. As well as protecting devices from attacks, also provides web protection powered by threat intelligence from SophosLabs and real-time intelligence from the Sophos Managed Detection and Response (MDR) team.

R;pple Browser Extension
Browser Extension installed across all school devices that "discretely intercepts harmful searches maintaining user privacy and signposts to free, 24/7 mental health support".

The DSL logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed every two years by the Assistant Headteacher responsible for online safety. At every review, the policy will be shared with the Governing Body. The review (such as the one available here) 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:

- Safeguarding and Child Protection Policy
- Behaviour Management Policy
- Staff disciplinary procedures
- Data Protection Policy and privacy notices
- Complaints Policy
- Acceptable Use Policy
- Searching, Screening and Confiscation Policy
- Policy on the Use of Reasonable Force and Other Restrictive Interventions
- Cyber Security Policy
- Social Media Policy