



The Ryleys

Girls & Boys Preparatory School

The Ryleys School E-Safety/ Online Policy

Monitoring: DSL

Named Person Responsible: S.Kirkbright

Reviewed: September 2026

Policy Review Date: September 2027

Scope

Our pupils are growing up in an increasingly complex world, living their lives seamlessly on and off line. This presents many positive and exciting opportunities, but also challenges and risks.

The use of the latest technology is actively encouraged at The Ryleys but with this comes a responsibility to protect both pupils and the school from abuse of the system.

What is the policy?

Online safety is an integral part of safeguarding. This Policy should be read alongside: the Statutory Framework for the EYFS; the Education and Skills Act 2008; the Children Act 1989; the Childcare Act 2006; the Data Protection Act 2018 and UK GDPR; the Equality Act 2010; Keeping Children Safe in Education 2026; DfE Behaviour Guidance; Teaching online safety in schools (DfE); Harmful online challenges and online hoaxes (DfE); Sharing nudes and semi-nudes: advice for education settings; and Relationships Education, Relationships and Sex Education (RSE) and Health Education (DfE). This Policy is also designed to sit alongside the school's Child Protection and Safeguarding Policy, Anti-Bullying Policy, Behaviour Policy and Staff Code of Conduct.

Governors' role and oversight

The Governors' role is to approve this Policy and review its effectiveness. They must satisfy themselves that the School has appropriate filtering and monitoring systems in place, reviewing their effectiveness regularly so as to demonstrate that the School is doing all it reasonably can to limit pupils' exposure to online risk. They hold regular reviews with the DSL, including consideration of online safety incident logs. They also support the School in engaging parents and the wider community in online safety.

Who is responsible?

The Designated Safeguarding Lead (DSL) will take lead responsibility for any online safety issues and concerns and follow the school's safeguarding and child protection procedures.

All staff have a responsibility to act as a good role model in their use of Technology and to share their knowledge of the School's policies and of safe practice with the pupils. Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding & Child Protection Policy.

The role of parents in ensuring that pupils understand how to stay safe when using Technology is crucial. The School expects parents to promote safe practice when using Technology and to:

- support the School in the implementation of this policy and report any concerns in line with the School's policies and procedures.
- talk to their child to understand the ways in which they are using the internet, social media and their mobile devices and promote responsible behaviour.
- encourage their child to speak to someone if they are being bullied or otherwise are concerned about their own safety or that of another pupil or need support.

If parents have any concerns or require any information about online safety, they should contact the school.

IT Support/Network Manager

The School's IT Support/Network Manager is One Education. They ensure that users may only access the School's network through an authorised, password-protected account, with passwords changed

at appropriate intervals. They maintain up-to-date virus and security protection. They ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. They ensure encryption and access controls protect personal and sensitive data held on School devices. They also report any misuse or attempted misuse of the network to the DSL for investigation.

Parent Engagement Programme

The School runs a rolling programme of information and guidance for parents, including: introduction of the Acceptable Use Agreement on entry; information on the systems used to filter and monitor pupils' online use, both in School and (where applicable) on School-issued devices at home; and talks, workshops or written guidance on safe internet use at home.

Assessment of risks

- The school currently does not allow pupils free access to mobile phones, iPads, Chromebooks and laptop computers this limits risks posed personally via global networks such as the internet.
- There is a secured wireless network within the school and this means the potential threat to security and access by unauthorised personal is minimised.
- Pupils access Chromebook laptops in the classrooms, through a secure, passworded connection to the school network.
- Staff have a username and passworded account, with access and allowance limitations imposed.
- The school internet service is firewalled and secured.
- Pupils have internet access within lessons, but games are limited to educational games that support the learning taking place in the classroom.
- Users are prevented from downloading executable files.
- All web activity is monitored and personal browsing histories kept.
- School web and email settings are set at the highest software security levels.
- In line with statutory guidance on mobile phones in schools, the School operates as a mobile phone-free environment by default. Pupils do not have access to personal mobile phones during the school day, including lessons, time between lessons, breaktimes, and lunchtime, except where an exception has been agreed by the Headteacher.
- The effectiveness of the School's filtering and monitoring systems is reviewed at least once every academic year. This review is carried out by the DSL with support from the SLT and IT support, and includes checks that filtering is working across all internet-connected devices and locations. A record of these checks is kept. Roles and responsibilities for managing filtering and monitoring are clearly assigned, and staff know how to escalate concerns identified through these systems.

Information and Cyber Security

The School takes measures to protect personal data and maintain appropriate cyber security, in line with the Department for Education's Cyber Security Standards for Schools and Colleges, as part of its wider safeguarding responsibilities.

Staff and Governor Training

The School provides all new staff, including those on placement or work experience, with induction training on this Policy and the Acceptable Use Agreement; makes regular CPD available to staff on emerging online safety issues, including AI-generated content and deepfakes; and ensures Governors

receive training sufficient to allow them to provide strategic challenge on the effectiveness of the School's online safety arrangements.

Digital Images, Video and Social Media

Parental consent for the taking and use of photographs and videos of pupils will be obtained on entry and reviewed annually. Consent will distinguish between use in public-facing materials (website, marketing, social media) and use in password-protected or School-only areas (parent portal, newsletters, displays). Pupils will not be identified by name alongside published images. Only School-owned equipment may be used to photograph or film pupils for School purposes. Parents and visitors attending School events may take photographs for personal use only and must not publish images featuring other people's children on social media without those parents' consent.

Education

The safe use of Technology is integral to the School's ICT curriculum. Pupils are educated in an age appropriate manner about the importance of safe and responsible use of Technology, including the internet, social media and mobile electronic devices.

Technology is included in the educational programmes followed in the EYFS in the following ways:

- Children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment.
- Children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology.
- Children are guided to recognise that a range of technology is used in places such as homes and Schools and encouraged to select and use technology for particular purposes.

Screen Use With Children

Babies and children under 2

- Screens are not used with children under 2, other than occasional supervised video calls with family members where this supports a child's wellbeing (for example, settling a child who is missing a parent).
- Passive screen time (television, tablets, background video) is not used with this age group.

Children aged 2 to 5

- Screen use is purposeful, adult-led, and directly linked to a specific learning objective (for example, listening to a short piece of music, viewing a small number of images to support a topic, or a brief, teacher-led interactive whiteboard activity).
- Screen-based activities are kept short, are never used to fill time, and are always balanced against active, hands-on and outdoor learning.
- Screens are not used as a reward or behaviour management tool.
- Where a screen is used with a group, an adult remains present throughout and actively engages with the children rather than leaving them to watch unsupervised.

Recording and Assessing Learning

- Staff may use setting-issued devices or approved learning journal platforms (e.g. Famly) to record observations, photographs and assessments of children's learning.
- Personal devices must never be used to photograph, film or record children under any circumstances.
- Any images or videos of children are taken on setting-issued devices only, uploaded promptly to the approved system, and deleted from the device once transferred.

The safe use of Technology is also a focus in all areas of the curriculum and key safety messages are reinforced as part of assemblies and tutorial/pastoral (P.S.H.E.) activities.

Lesson and activities are designed to teach pupils:

- About the risks associated with using the Technology and how to protect themselves and their peers from potential risks.
- To be critically aware of content they access online and guided to validate accuracy of information. How to recognise suspicious, bullying, radicalisation and extremist behaviour.
- The definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect.
- The consequences of negative online behaviour.
- How to report cyberbullying and/or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

The Ryleys computer system provides internet access to pupils and staff. This RUIS will help protect pupils, staff and the School by clearly stating what is acceptable and what is not.

Responsible Internet Use Statement (RIUS)

1. Access must only be made via the user's authorised account and password, which must not be given to any other person.
2. School computer and internet use must be appropriate to the pupil's academic education or to staff professional activity.
3. Copyrights and intellectual property rights must be respected.
4. Users are responsible for emails they send and for contacts made.
5. Emails should be written carefully and politely. As messages may be forwarded, email is best regarded as public property.
6. Anonymous letters and chain mail must not be sent or forwarded.
7. The use of public chat rooms is not allowed.
8. Only games to enhance lessons may be used during school hours.
9. No internet games may be freely accessed.
10. Only use the URL bar with staff permission.
11. Users must log off after use, do not leave a computer logged in and unattended.

Email Rules

- Never reply to unpleasant or unwanted emails.
- Never give your email address to anyone except close family and friends.
- Don't accept emails or open files from people you do not know.
- Do not click on any links or open any email into the full window if you are unsure of the sender or content.
- Visit www.thinkuknow.co.uk to ensure you know how to be safe.
- Report abuse at www.ceop.gov.uk/
- Childline/IWF's Report Remove tool (childline.org.uk) helps children get a nude image removed from the internet.

Web Rules

- Do not use the URL bar unless permission is given.
- Do not click on links unless you are certain what they are.

- Report to a teacher if you find a dubious web page as this will appear in your history.

Report any concerns immediately. www.thinkuknow.co.uk and www.ceop.gov.uk/

In addition to speaking to a trusted adult, younger pupils may raise online safety or wellbeing concerns through the School's worry / sharing boxes which are monitored by individual class teachers.

Procedures for dealing with incidents of misuse

Staff, pupils and parents are required to report incidents of misuse or suspected misuse, including incidents of sexual harassment via mobile or smart tech, to the School in accordance with this policy and the School's safeguarding and disciplinary policies and procedures. All incidents will be dealt with in line with the above policies.

The School's filtering system is Sophos Firewall and the monitoring system is Senso. All online safety incidents, together with associated actions, are logged on CPOMS using an 'Online Safety' tag, and contribute to the School's ongoing review of policy and practice.

The following incidents require immediate referral to the DSL: any incident involving AI-generated sexual imagery; online sexual harassment between pupils; content indicating a risk of radicalisation or extremism; and gambling or gaming-related concerns suggesting addiction or financial harm. The DSL acts as the first point of contact for online safety concerns; complaints about staff misuse are referred directly to the Head.

Misuse by pupils

- Anyone who has any concern about the misuse of Technology by pupils should report it so that it can be dealt with in accordance with the School's behaviour and discipline policies, including the Anti-Bullying Policy where there is an allegation of cyberbullying.
- Anyone who has any concern about the welfare and safety of a pupil must report it immediately in accordance with the School's child protection procedures (see the School's Safeguarding & Child Protection Policy).

Misuse by staff

- Anyone who has any concern about the misuse of Technology by staff should report it in accordance with the School's Whistleblowing Policy so that it can be dealt with in accordance with the staff disciplinary procedures.
- If anyone has a safeguarding-related concern, they should report it immediately so that it can be dealt with in accordance with the procedures for reporting and dealing with allegations of abuse against staff set out in the School's Safeguarding & Child Protection Policy.

If the School considers that any person is vulnerable to radicalisation the School will refer this to the Channel programme. This focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism. Any person who has a concern relating to extremism may report it directly to the police.

Online Safety

Managing Online Risks

Online safety is an integral, evolving part of safeguarding. Risks change as technology changes, and the School's approach is reviewed at least annually to reflect this.

In line with Keeping Children Safe in Education 2026, online safety risks are categorised into four areas:

- **Content** — being exposed to illegal, inappropriate, or harmful material, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news), and conspiracy theories.
- **Contact** — being subjected to harmful online interaction with other users, or with generative AI applications that simulate this, such as peer-to-peer pressure, commercial advertising, or adults posing as children or young people with the intention to groom or exploit them for sexual, criminal, financial, or other purposes.
- **Conduct** — online behaviour that increases the likelihood of, or causes, harm, such as making, sending, or receiving explicit images (including those generated using AI), and online bullying.
- **Commerce** — risks such as online gambling, inappropriate advertising, phishing, and financial scams. Suspected phishing affecting pupils, or staff should be reported to the Anti-Phishing Working Group ([apwg.org](https://www.apwg.org)).

These four areas evolve at different stages of a child's development, so vulnerability to online harm is not fixed — it depends on age, circumstances, and online behaviour, and can change over time. No single group of children is 'the' vulnerable group; the School remains alert to risk for all pupils, adjusting its approach as pupils grow and technology changes.

Generative AI

The School recognises that generative AI tools present both opportunities and risks, including the potential for AI-generated harmful or explicit content. Staff and pupils' use of generative AI is subject to this policy and to the School's filtering and monitoring systems. Guidance on the safe use of generative AI in education, including data protection, safeguarding, and intellectual property considerations, is available from the Department for Education.

What We Can Do as Parents and Staff

- Take an active interest in what children are doing online and which devices and apps they use.
- Talk with children regularly about their online activity, without judgement.
- Use parental controls where appropriate and understand the School's filtering and monitoring arrangements.
- Encourage children to tell a trusted adult if anything online makes them uncomfortable.

What We Teach Children and Young People

- To protect personal information (address, phone number, school, passwords) and manage privacy settings.
- To be aware that devices can share location and other information without their knowledge, and how to control this.
- To limit time online and balance it with offline activity.
- Never to arrange to meet an online-only contact in person, and to tell an adult if someone tries to arrange this.
- To speak up if something online upsets or worries them, and that not everything online is true.
- Never to do or say anything on a webcam or video call they would not want made public.
- To think carefully before sharing their location, and to check privacy settings on apps and games.
- To recognise scam emails, suspicious downloads, and the risks of illegal downloading or

file-sharing.

- That everyone has a role in keeping each other safe online.

RSE and Online Safety Integration

Online safety education is closely integrated with Relationships and Sex Education. Pupils learn that online friendships and interactions should follow the same principles of kindness and respect as face-to-face relationships; that private body parts remain private online and offline, and should never be shared or requested; and how to recognise when online communication makes them feel uncomfortable, and who to tell.

Guidance on Online Bullying, for Pupils

Don't respond or retaliate. Talk to a trusted adult. Save the evidence. Block the person involved. Be a friend, not a bystander — and don't be a bully yourself.

Guidance for Staff and Parents Responding to Online Bullying

Listen and take the child seriously. Make sure they are, and feel, safe. Don't overreact, and don't encourage retaliation. Gather the facts and preserve evidence. Involve the child in working out next steps. Support their self-esteem and resilience. Loop in the School if there is a link to it.