

The Richard Pate School



Cyber-Bullying Policy

September 2026 JMH LK

This is a whole school policy and applies to EYFS

This policy should be read in conjunction with the Anti-bullying Policy, the Behaviour Policy, the Safeguarding and Child Protection Policy (including Prevent) and the Code of Conduct.

It should also be read alongside the school's Online Safety/Acceptable Use arrangements, Filtering and Monitoring procedures and relevant data protection policies.

The school recognises that a bullying incident should be treated as a child protection concern when there is reasonable cause to believe that a child is suffering or likely to suffer significant harm.

All concerns about online behaviour must be considered from a safeguarding perspective. Child-on-child abuse can take place inside or outside school and online, and concerns must be reported to the Designated Safeguarding Lead (DSL) or a deputy without delay.

Cyberbullying

Cyberbullying may be defined as the use of digital technology or online communications to bully, harass, threaten, humiliate or otherwise harm another person. It may occur through messaging, social media, gaming, online platforms, apps, email, images, video, live-streaming, artificial intelligence (AI) tools or other digital services.

It can take a number of different forms:

- threats and intimidation,
- harassment or 'cyber-stalking' (e.g. repeatedly sending unwanted texts or instant messages), consensual or non-consensual sharing of nudes and semi-nudes, including self-generated intimate images and images generated or manipulated using AI, such as deepfakes,
- vilification/defamation, exclusion/peer rejection,
- impersonation,
- unauthorised publication of private information/images
- 'trolling' (abusing the internet to provoke or offend others online)
- the creation, alteration or circulation of harmful, sexualised, misleading or abusive AI-generated content, including deepfakes.

It can be an extension of face-to-face bullying, with technology providing the bully with another route to harass their target.

However it differs from other forms of bullying in several significant ways:

- by facilitating a far more extreme invasion of personal space. Cyberbullying can take place at any time and intrude into spaces that have previously been regarded as safe and personal.
- the potential for anonymity on the part of the person responsible. This can be extremely distressing for the target.
- the potential for content to reach a large audience very rapidly, so the scale and scope of cyberbullying can be greater than for other forms of bullying.
- once content is shared online it can be difficult to control, copy or remove, which can amplify the impact on the child.
- by forwarding, reposting, liking, sharing or otherwise amplifying humiliating or abusive material, bystanders may contribute to the harm.
- cyberbullying can take place between peers and across generations. Staff can also be victims.
- online incidents can provide evidence. Staff and pupils should preserve relevant information safely, but must not view, copy, print, download or share nude or semi-nude images of children.

Cyberbullying and the Law

Bullying is never acceptable and the school fully recognises its duty to protect all of its members and to provide a safe, healthy environment for everyone.

Education Law:

- The Education and Inspections Act 2006 (EIA 2006) outlines some legal powers which relate more directly to cyberbullying. Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off the school site.
- Staff may confiscate, retain or dispose of pupils' property in circumstances permitted by law and the school's Searching, Screening and Confiscation procedures. Any search of an electronic device must be undertaken in accordance with current DfE guidance and safeguarding procedures.

Civil and Criminal Law

There is no single criminal offence of cyberbullying. Depending on the circumstances, online conduct may engage a range of legislation, including the Protection from Harassment Act 1997, Malicious Communications Act 1988, Communications Act 2003, Computer Misuse Act 1990, Sexual Offences Act 2003, Online Safety Act 2023 and other relevant criminal or civil law. The school will seek advice from the police or other agencies where appropriate.

The creation, possession or distribution of indecent images of a child can constitute a criminal offence. Incidents involving nudes and semi-nudes will be managed in accordance with current UK Council for Internet Safety guidance and the school's Safeguarding and Child Protection Policy.

Preventing Cyberbullying

As with all forms of bullying, the best way to deal with cyberbullying is to prevent it happening in the first place.

There is no single solution to the problem of cyberbullying but the school will do the following as a minimum to impose a comprehensive and effective prevention strategy:

Online safety is considered as part of the school's whole-school safeguarding approach. The school recognises the four broad areas of online risk: content, contact, conduct and commerce, and will ensure that pupils are taught how to recognise, manage and report these risks.

Roles and Responsibilities

The Head and Deputy Head (Pastoral), who is also the Designated Safeguarding Lead will take overall responsibility for the co-ordination and implementation of cyberbullying prevention and response strategies.

The Head and Deputy Head (Pastoral) will :

- ensure that all incidents of cyberbullying both inside and outside school are dealt with immediately and will be managed and/or escalated in line with the procedures set out in the school's Anti-bullying Policy, Behaviour Policy and Safeguarding and Child Protection Policy.
- ensure that all policies relating to safeguarding, including cyberbullying are reviewed and updated regularly.
- ensure that all staff know that they need to report any issues concerning cyberbullying, child-on-child abuse or other online harms to the Designated Safeguarding Lead.
- ensure that all staff are aware of the Prevent Duties.
- provide training so that staff feel confident to identify children at risk of being drawn into terrorism, to challenge extremist ideas and to know how to make a referral when a child is at risk. The DSL is also the Designated Prevent Lead.
- ensure that parents/carers are informed and attention is drawn annually to the cyberbullying policy so that they are fully aware of the school's responsibility relating to safeguarding pupils and their welfare.

The Cyberbullying Policy is available at all times on the school website:

- ensure that at the beginning of each term, cyberbullying is revisited as part of the Staying Safe Programme and that pupils know how to report a concern.
- ensure that all staff are aware of their responsibilities by providing clear guidance for staff on the use of technology within school and beyond. All staff should sign to say they have read and understood the Staff Code of Conduct.
- ensure that all staff read Part One of Keeping Children Safe in Education 2026 and receive safeguarding and child protection updates, including online safety, as required.

The Heads of Computing, PSHE, RSHE, Curriculum Lead and Designated Safeguarding Lead will:

- ensure that all pupils receive clear, age-appropriate guidance on the safe and positive use of technology in school and beyond, including privacy, personal data, respectful relationships, misinformation, AI-generated content and how to report abuse or bullying online.
- ensure the school's Acceptable Use Policy, Guidelines for Staff when Children are using Digital Devices and Children's Use of Digital Devices are reviewed at least annually and when significant new technology or safeguarding risks are introduced.

- provide annual training for staff on the above policies and procedures.
- provide annual training for staff on online safety.
- plan and deliver an age-appropriate online safety curriculum through computing, PSHE/RSHE and the wider curriculum that develops pupils' digital resilience, critical thinking and ability to recognise and report harmful content, contact, conduct and commercial risks.
- ensure pupils are taught about the risks associated with generative AI, including inaccurate or harmful outputs, impersonation, deepfakes, privacy, data protection and the inappropriate creation or sharing of sexualised or abusive content.

The Network Manager will:

- maintain appropriate filtering and monitoring systems and work with the DSL and senior leadership to identify and respond to safeguarding concerns. Filtering and monitoring will take account of illegal, inappropriate and potentially harmful content in text, image, audio, video and AI-generated formats.
- ensure filtering is active and appropriately configured for school-managed devices and services, including devices used off-site, and for users of the school network. Where relevant, systems should address technologies used to circumvent filtering, such as VPNs and proxy services.
- provide filtering and monitoring reports and urgent/high-risk alerts to the DSL in a form that enables prompt safeguarding action and maintain records of technical checks and actions taken.
- work with senior leaders, the DSL and the responsible trustee to review filtering and monitoring provision at least once every academic year and following significant safeguarding risks, new technology (including generative AI), major software updates or material changes to the network or devices. The review and resulting actions will be recorded.
- ensure monitoring arrangements include appropriate regular reporting, with immediate escalation of high-risk safeguarding concerns, and that users are informed that school systems and devices are filtered and monitored.
- ensure that visitors to the school are given clear guidance on the use of technology in school. This includes how to report any safeguarding issues to the Designated Safeguarding Lead. Visitors will be given highly restricted guest accounts which will not allow any access to personal data and that any misuse of the system will result in access to the system being withdrawn.
- although children will not have access to ai sites, the newtwork manager will support the completion and review of appropriate data protection impact assessments and privacy information for filtering, monitoring, AI and other educational technology where required.

The Bursar will

- ensure the school manages personal data in line with statutory requirements. The school is aware of its duties under the Data Protection Act (1998). Careful consideration will be given when processing personal information so that the individual's privacy is respected where it needs protection. Access to the personal information will only be given to those who need it. The principles of the Data Protection Act will be applied when processing, collecting, disclosing, retaining or disposing of information relating to a pupil or member of staff.

The School Trustees will

- appoint a trustee in charge of welfare who will work with the Designated Safeguarding Lead to ensure the policies and practices relating to safeguarding including the prevention of cyberbullying are being implemented effectively. The current trustee for safeguarding is Sue Wade.

Guidance for Staff

Guidance on safe practice in the use of electronic communications and storage of images is contained in the Code of Conduct. The school will deal with inappropriate use of technology in line with the Code of Conduct which could result in disciplinary procedures.

If you suspect or are told about a cyberbullying or other online safeguarding incident or have a concern, act immediately, listen to the child, avoid promising confidentiality, record the concern accurately on the Online Concern Report Form and report it to the DSL or a deputy without delay. Do not investigate the matter yourself beyond what is necessary to establish the immediate safeguarding concern.

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Computers

Where appropriate, ask the pupil to show you the material without unnecessarily searching through other content.

Preserve relevant evidence such as URLs, usernames, dates, times and messages where it is safe and lawful to do so.

Do not print, copy, download, forward or save nude or semi-nude images of a child. Do not ask a child to send or share such an image with you. Refer the matter immediately to the DSL.

Do not delete material unless directed to do so by the DSL, police or other appropriate agency, except where leaving material accessible would create an immediate safeguarding risk.

Inform the DSL or a deputy immediately and pass on the information you have.

The DSL will decide what further action, risk assessment, recording, parental contact, referral or agency involvement is required in line with safeguarding procedures.

Mobile Phones

Children are not allowed to bring mobile phones or devices into school unless they have sought permission from the headmaster and permission has been agreed in writing. If permission has been granted, devices are to be switched off and immediately handed into a member of staff when the child enters school. Devices will be locked away until the end of the child's school day and then handed back to the child.

Should a pupil receive a cyberbullying incident on a mobile phone out of school, we recommend that parents

- ask the pupil to show them the relevant content, while avoiding unnecessary viewing or sharing.
- record relevant details such as the date, time, platform, usernames and nature of the content. Adults and staff must not view, copy, print, download or forward nude or semi-nude images of a child.

- make a written note of any relevant spoken or voice message, including dates, times and names where known.
- preserve relevant evidence, but do not ask the child to re-share sexual imagery or other illegal material.
- inform the Designated Safeguarding Lead as soon as possible and provide the relevant information.
- where there is an immediate risk of harm, contact the police or emergency services as appropriate

Use of Technology in School

All members of the school community are expected to take responsibility for using technology positively.

As well as training, the following is in place:

- All staff are expected to sign to confirm they have read and understood the Acceptable Use Policy.
- All staff are expected to sign to confirm they have read and understood the Staff Code of Conduct.
- All staff are expected to have read and understood Guidelines for Staff when Children are using Digital Devices.
- All children are expected to have been taken through and understood Children's Use of Digital Devices.
- Pupils are not permitted to access generative AI services at school unless a specific tool or activity has been formally approved by the school. Attempts to bypass filtering or monitoring controls must be reported and treated as both a technical and, where appropriate, safeguarding concern.
- Any school-approved use of generative AI will be risk assessed and subject to appropriate safeguarding, filtering, monitoring, privacy and data protection controls.

This is a whole school policy

Guidance for Pupils

If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, or a member of staff on your safety network. You will be listened to and taken seriously.

- Do not reply to abusive messages. Save or record relevant information and report it to a trusted adult.
- Do not delete relevant evidence until a trusted adult has helped you decide what to do, unless keeping it would expose you or someone else to further harm.
- Never save, screenshot, forward or share a nude or semi-nude image of a child. Tell a trusted adult immediately.
- Do not give out personal details or contact information without the permission of a parent/carer.
- Be careful who you connect with online and think about what information you allow others to see.

- Protect your passwords and passcodes. Do not share them with other pupils and use strong, unique passwords where possible.
- Always log off or lock a device when you have finished or leave it unattended.
- Use privacy and safety settings and ask a trusted adult if you are unsure how to use them.
- Do not respond to abusive messages or contact from people you do not know. Block and report accounts where appropriate.
- Do not try to bypass the school's filtering or monitoring systems, including by using VPNs, proxy sites or other workarounds.
- Do not use AI tools to impersonate, embarrass, sexualise, threaten or harm another person, or to create or alter images of them without appropriate permission.
- Remember that AI-generated information can be inaccurate, biased or unsafe. If something online worries or confuses you, speak to a trusted adult.
- The school will deal with cyberbullying in the same way as other bullying. Do not think that because it is online it is different to other forms of bullying.
- The school will deal with inappropriate use of technology in the same way as other types of inappropriate behaviour and sanctions will be given in line with the school's Behaviour Policy.

Guidance for Parents/Carers

It is vital that parents/carers and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. Parents/carers are encouraged to take an active, age-appropriate interest in their child's online life and to maintain open conversations about online safety.

- Parents/carers can help by making sure their child understands the school's policy and how seriously the school takes cyberbullying and online safeguarding concerns.
- Parents/carers should discuss safe and respectful online behaviour, privacy, the sharing of images, misinformation, scams, harmful content and the risks associated with AI-generated content and deepfakes.
- If parents/carers believe their child is the victim of cyberbullying, they should preserve relevant information such as messages, URLs, usernames, dates and times where safe to do so. They should not copy, print, download or forward nude or semi-nude images of a child.
- Parents/carers should contact the school as soon as possible. Please contact Mrs Miller-Howell jmiller-howell@richardpate.co.uk
- If the incident falls in the holidays the school reserves the right to take action against bullying perpetrated outside the school both in and out of term time.

The school will ensure parents/carers are informed of the cyber-bullying policy and cyberbullying leaflet for children and the procedures in place in the Anti-Bullying Policy to deal with all forms of bullying including cyber-bullying.

E-Safety at Home

Parents/carers are encouraged to use current, reputable online safety guidance and to talk regularly with their child about what they do online. Helpful sources include the UK Safer Internet Centre, Childnet, Internet Matters, CEOP Education and the NSPCC.

Parents/carers should be aware that filtering and parental controls can reduce risk but cannot remove it entirely. Open communication, age-appropriate supervision and clear family expectations remain important.

Review and Reference Guidance

This policy has been reviewed with reference to Keeping Children Safe in Education 2026, the Department for Education Filtering and Monitoring: Core Standard (updated August 2026), DfE Generative AI Product Safety Standards, and UKCIS guidance on sharing nudes and semi-nudes. ISBA member guidance should also be checked at each review to ensure any current independent-school-specific recommendations are incorporated.

The policy will be reviewed at least annually and sooner where there is a significant safeguarding incident, a material change in technology or working practice, new statutory guidance, or a significant change to filtering and monitoring arrangements.

Several sites offer helpful advice to parents/carers, particularly with respect to how they can best monitor their child's use of the computer at home. Here are some parents/carers might like to try:

- www.thinkuknow.co.uk/parents
- www.saferinternet.org.uk
- www.childnet.com
- www.anti-bullyingalliance.org.uk
- www.nspcc.org.uk
- DfE Advice for Parents on Cyberbullying

- Childnet Cyberbullying Leaflet

- DfE The use of social media for on-line radicalisation

The Designated Safeguarding Lead is: Jacqueline Miller-Howell Head, Deputy Head (Pastoral) Tel: 01242 522083 jmiller-howell@richardpate.co.uk

The EYFS Designated Safeguarding Lead is: Paula Hunte



THE RICHARD PATE SCHOOL

RPS ONLINE SAFEGUARDING CONCERN : Staff reporting form

IMPORTANT: If a child may be at immediate risk of harm, speak to the DSL/Deputy DSL immediately. Do not rely on this form alone.

1. CHILD / CHILDREN INVOLVED

Child's name: _____

Year/Class: _____

Other children involved _____

Date concern identified: _____ Time: _____ Staff member reporting: _____

2. HOW DID THE CONCERN COME TO YOUR ATTENTION?

- | | | |
|--|---|---|
| ☐ Child told me | ☐ Staff member reported it | ☐ Parent/carer reported it |
| ☐ I witnessed it | ☐ Filtering/monitoring alert | ☐ Seen/heard during a lesson |
| ☐ Another child reported it | ☐ Seen on a school device | |
| ☐ Other: _____ | | |

3. WHAT TYPE OF ONLINE CONCERN IS THIS?

Tick any that apply.

- | | |
|---|---|
| ☐ Upsetting/inappropriate content | ☐ Sexual content or sexualised behaviour |
| ☐ Online bullying/unkind behaviour | ☐ Threats, harassment or intimidation |
| ☐ Sharing/requesting images | ☐ Contact with an unknown person |
| ☐ Grooming/exploitation concern | ☐ Social media/messaging |
| ☐ Gaming/chat platform | ☐ Self-harm/suicide-related content |
| ☐ Hate/discriminatory content | ☐ Radicalisation/extremism concern |
| ☐ Online challenge/risky behaviour | ☐ Privacy/personal information |
| ☐ Filtering or monitoring concern | ☐ Attempt to bypass school filtering |
| ☐ Generative AI/AI-generated content concern | |
| ☐ Other: _____ | |

4. WHAT HAPPENED?

Record facts, not assumptions. Where a child has spoken to you, record their words as accurately as possible:

Website/app/platform/device involved (if known):

What happened / what was seen, heard or disclosed?

When and where did the incident happen?

Was this on:

☐ School device/network ☐ At school ☐ Unknown ☐ At home ☐ Personal device

5. IMMEDIATE SAFETY

Is there any indication that a child may be at immediate risk? ☐ Yes ☐ No

☐ Unsure

Does the concern involve an adult or unknown online contact? ☐ Yes ☐ No

☐ Unsure

Has content/image/video been shared with others? ☐ Yes ☐ No

☐ Unsure

Immediate action taken:

6. EVIDENCE / INFORMATION

☐ URL/web address recorded ☐ Username/account recorded
☐ Filtering/monitoring alert available ☐ Relevant message/post identified ☐ Other:

Do not investigate the child's device or ask the child to search for, forward or reproduce harmful/sexual content. Seek DSL advice.

7. REPORT TO DSL

Reported to: _____ **Date:** _____

Time: _____

☐ Spoken to DSL/Deputy DSL directly ☐ Safeguarding recording system updated
☐ Both

Signature/name of reporting member of staff:

DSL / DEPUTY DSL SECTION

Risk assessment / safeguarding considerations:

Actions taken:

- | | | |
|---|--|---|
| ☐ Child spoken to
child/children considered | ☐ Parent/carers contacted | ☐ Other |
| ☐ IT support involved
arranged | ☐ Filtering/monitoring investigated | ☐ Pastoral support |
| ☐ Early Help considered
consulted/contacted | ☐ Children's Social Care consulted/referred | ☐ Police |
| ☐ CEOP/reporting route considered | ☐ Other agency involved | |
| ☐ No further safeguarding action required | | |
| ☐ Other: _____ | | |

Decision and rationale:

Outcome / follow-up required:

Review date (if required): _____

DSL/Deputy DSL: _____ **Date:** _____