

Online Safety Policy



Person Responsible for Policy:
Claire McKinney (Head Teacher)

Date of Adoption by Governing Body:
Autumn 2026

Date of next review:
Autumn 2027

Online safety is an integral part of safeguarding

It is designed to sit alongside the school's Child Protection policy.

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

This policy aims to:

- Help all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, and regardless of device or platform
- Facilitate the safe, responsible and respectful use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of today's and tomorrow's digital world, to survive and thrive online
- Help school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

- for the protection and benefit of the children and young people in their care
- for their own protection, minimising misplaced or malicious allegations
- for the benefit of the school, supporting the school ethos, aims and objectives, and protecting the reputation of the school and profession
- Establish clear structures by which online misdemeanours will be treated, and procedures to follow where there are doubts or concerns

The term Internet Safety includes the following areas:

1. Anti Cyber bullying
2. School Internet Access and E Safety
3. Website
4. Social Media
5. AI

1. Anti Cyber Bullying

This school believes that all people in our community have the right to teach and learn in a supportive, caring and safe environment without fear of being bullied. We believe that every individual in school has a duty to report an incident of bullying whether it happens to themselves or to another person.

Definition

There are many types of cyber-bullying. Although there may be some of which we are unaware, here are the more common.

- **Text messages** - that are threatening or cause discomfort
- **Picture/video-clips via mobile phone cameras** - images sent to others to make the victim feel threatened or embarrassed.
- **Mobile phone calls** - silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
- **Emails** - threatening or bullying emails, often sent using a pseudonym or somebody else's name.

- **Chatroom bullying** - menacing or upsetting responses to children or young people when they are in a web-based Chatroom.
- **Instant messaging (IM)** - unpleasant messages sent while children conduct real-time conversations online using online chat mediums.

At Richard Avenue Primary School, we take this bullying as seriously as all other types of bullying and, therefore, will deal with each situation individually. An episode may result in a simple verbal warning. It might result in a parental discussion. Clearly, more serious cases will result in further sanctions.

At Richard Avenue Primary School, pupils are taught how to:

- Understand how to use these technologies safely and know about the risks and consequences of misusing them as well as taking part in eSafety lessons
- Know what to do if they or someone they know are being cyber bullied. Report any problems with cyber bullying. If they do have a problem, they can talk to the school, parents, or the police to do something about it.

Richard Avenue Primary School has:

- Information for parents on: Standards and practices in schools, what to do if problems arise, what's being taught in the curriculum.
- Support for parents and pupils if cyber bullying occurs by: assessing the harm caused, identifying those involved, taking steps to repair harm and to prevent recurrence.

2. School Internet Access and E Safety

Authorisation of Internet access

The school will allocate access to the Internet on the basis of educational needs. Internet access is a necessary part of planned lessons. It is an entitlement for pupils based on responsible use:

- At Key Stage 1, access to the Internet will be by teacher or adult;

- At Key Stage 2, Internet access will be granted to a whole class as part of the scheme of work, after a suitable introduction to the rules for responsible Internet use.

Maintenance and security of the school ICT system

- The ICT Technician will ensure that the system has the capacity to take increased traffic caused by Internet use,
- The security of the whole system is up to date to deal with threats to security from Internet access,
- Virus protection is installed and updated regularly by the technician;
- Personal USB or external drives are not permitted on the school network

Ensuring Internet use provides effective learning

- Internet access will be planned to enrich and extend learning activities as an integrated aspect of the curriculum;
- Pupils will be given clear objectives for Internet use;
- Pupils will be provided with lists of relevant and suitable websites, pupils will be educated in taking responsibility for Internet access;
- Pupils will be informed that checks can be made on files held on the system;
- The school will work with the LA, as the Internet Service Provider, to ensure systems to protect pupils are reviewed and improved.

Education and Training

Richard Avenue recognises that the internet and other digital technologies can transform learning; help to improve outcomes for children and young people; promote creativity; all of which add up to a more exciting and challenging classroom experience.

As part of achieving this, we want to create within Richard Avenue an accessible system, with information and services online, which support personalised learning and choice.

However, we realise that it will be necessary for our pupils to have the skills of critical awareness, digital literacy and good online citizenship to enable them to use the internet and other digital technologies safely. When accessing online materials children should consider the following questions:

- Is this website/URL/email fake? How can I tell?
- Is this person who they say they are?
- Why does someone want me to see this?
- Why does someone want me to send this?
- Why would someone want me to believe this?
- Why does this person want my personal information?
- Is this too good to be true?
- Is this fact or opinion?

To this end, Richard Avenue will:-

- Enable all pupils to exercise the skills of critical awareness, digital literacy and good online citizenship as part of the school curriculum. This is provided as part of Computing, PSHE, assemblies and other relevant subjects/pastoral lessons.
- Educate school staff so that they are equipped to support pupils in gaining positive experiences when online and can help pupils develop strategies if they encounter a problem.
- Educate pupils to acknowledge the source of information used and to respect copyright using materials accessed on the internet.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use.

Management of E-mail

Due to the simplicity and low cost of E-mail, care needs to be taken that there are no adverse consequences to the school, or to the pupil, through such messages. Once available, it is

difficult to control the content of E-mail without compromising privacy.

- Pupils are expected to use E-mail as part of the Computing curriculum. Children will use the secure emailing system provided to them by the ICT technician;
- Communications with persons and organisations will be managed restricted to the boundaries of the school;
- Pupils may send E-mail as part of planned lessons and will be given individual e-mail accounts.

3. Website

Management of publishing on the Web

- The Headteacher will delegate editorial responsibility to the ICT Technician to ensure that content is accurate and quality of presentation is maintained
- Pupils will be taught to publish for a wide range of audiences- which might include governors, parents or younger children.
- The point of contact on the Website will be the school's address and telephone number. Home information or individual E-mail identities will not be published;
- No names of any child will be attached to photographs published onto the internet.
- With regards to children, only group photos will be published on the website.

Ensuring Internet access is appropriate and safe

Pupils in school are unlikely to see inappropriate content in books due to selection by publisher and teacher. Staff will need to ensure that access is appropriate to the user. Teachers will need to research areas including drugs, medical conditions, bullying or harassment.

- Staff will check that the sites selected for pupil use are appropriate to the age and maturity of pupils;
- Staff will monitor the effectiveness of Internet access strategies;

- Access levels will be reviewed as pupils' Internet use expands and their ability to retrieve information develops;

Staff are best placed to make their own decisions about which resources are educationally appropriate for their pupils. This includes reviewing resources, even when from a trusted source, as some will be more appropriate to their cohort of pupils than others.

Staff should ask themselves:

- Where does this organisation get their information from?
- What is their background?
- Are the resources age appropriate for our pupils?
- Are the resources appropriate for the developmental stage of our pupils?

Handling inappropriate use/complaints

Prompt action will be required if a complaint is made. The facts of the case will need to be established, for instance it is possible that the issue has arisen through home Internet use or by contacts outside school. Transgressions of the rules by pupils could include minor as well as the potentially serious sanctions. Sanctions for irresponsible use will be linked to the schools behaviour policy.

- Responsibility for handling incidents will be given to a senior member of staff;
- Pupils and parents will be informed of the procedure;
- Parents and pupils will need to work in partnership with staff to resolve any issue;
- The ICT coordinator will be notified. If staff or pupils discover unsuitable sites, the URL (address) and content will be reported to the LA as Service Provider through the ICT Technician;
- A pupil may have Internet or computer access denied for a period.

How will staff, pupils and parents be kept informed?

- Rules for Responsible Internet access will be posted near all computer systems.
- All staff including teachers, supply staff, classroom assistants and support staff, will be provided with the Internet Access Policy, and its importance explained;
- Parents' attention will be drawn to the Policy on the school website

4. Social Media

The aim of this section is to give clarity to the way in which social media sites are to be used by the staff and children of Richard Avenue Primary school. All members of the school community should bear in mind that information they share through social media and networks, even if it is in private spaces, is still subject to UK libel and defamation laws.

The use of social media sites by pupils whilst at school

A. Pupils should not access social networking sites whilst at school.

Pupils and parents should be reminded that the use of some social media sites is inappropriate for Primary aged children and illegal for others.

B. Use of social media sites by employees in a personal capacity.

It is important that staff protect their professional reputation, and that of the school, by ensuring that they use their personal sites in an appropriate manner.

Staff are advised as follows:

- Staff should familiarise themselves with social network sites' privacy settings in order to ensure that information is not automatically shared with a wider audience than intended.
- That they do not conduct or portray themselves, or allow friends to portray them, in a manner which may:

- Bring the school into disrepute;
- Lead to valid parental complaints;
- Be deemed as derogatory towards the school and/or its employees;
- Be deemed as derogatory towards pupils, parents/carers or governors;
- Bring into question their appropriateness to work with children;
- Contravene current National Teacher Standards.
- That they do not form online friendships or enter into communication with parents/carers as this could lead to professional relationships being compromised.
- That they do not form online friendships or enter into online communication with pupils as this could lead to professional relationships being compromised, and/or safeguarding allegations being raised.
- That they should not post pictures of or negative comments about school events.
- That if their use of social media/networking sites contravenes this policy, they may be subject to disciplinary action.

C. Creation of social media accounts by school staff for use in education.

All social media services must be approved by the Head teacher in advance of any educational work being undertaken.

D. Comments posted by parents/carers on social media sites

Parents/carers will be made aware of their responsibilities regarding their use of social media via this policy (in particular when their child joins the school), the school website, letter and school newsletters.

- Parents/carers are asked not to post images (photos and videos) of pupils other than their own children on social media sites unless they have the permission of parents of other children pictured.

- Parents/carers are asked to raise queries, concerns or complaints directly with the school rather than posting them on social media.
- Parents/carers should not post malicious or fictitious comments on social media sites about any member of the school community.

5. Artificial Intelligence

Purpose & Scope

This policy outlines the appropriate, safe, and ethical use of Artificial Intelligence (AI) tools at Richard Avenue. It applies to all staff, pupils, contractors, and visitors using school-owned hardware, personal devices on school networks, or representing the school in any digital capacity.

Key Risks & Dangers of AI

While AI offers valuable educational support, the school recognizes significant risks associated with its misuse:

- **Data Privacy & GDPR Breaches:** Exposing confidential staff, pupil, or operational data to external AI training models.
- **Safeguarding & Harmful Content:** Exposure to, or creation of, inappropriate materials, deepfakes, or harassment.
- **Hallucinations & Misinformation:** Relying on unverified, inaccurate, or biased AI outputs for teaching or learning.
- **Over-reliance & Skill Atrophy:** Impairing critical thinking, writing, and analytical skills through passive reliance on automation.

Staff

Acceptable Use

- **Lesson & Resource Creation:** Generating draft lesson frameworks, worksheets, or creative ideas.
- **Administrative Tasks:** Drafting generic letters, summarizing non-sensitive text, or generating ideas for extracurricular events.

Prohibited & High-Risk Actions

- **Zero Personal Data:** Staff **must never** input Personally Identifiable Information, medical records, safeguarding notes or individual pupil work containing names into unapproved AI tools.
- **Automated Grading:** AI must not be used to make final grading, assessment, or pastoral care decisions without direct human review.
- **Unverified Output:** Staff are fully responsible for any AI-assisted material they use or send. All AI outputs must be checked for factual accuracy, bias, and appropriateness prior to publication.

Pupil Guidelines

Acceptable Use

- **Supervised Learning:** Using school-approved AI platforms for guided research, brainstorming, or learning assistance as explicitly instructed by a teacher.

Prohibited Actions

- **Plagiarism:** Submitting AI-generated answers, or projects as original work is strictly prohibited and treated as academic misconduct.
- **Deepfakes & Harassment:** Generating or modifying audio, images, or videos of staff or fellow pupils is a severe breach of school safety.
- **Bypassing Filters:** Attempting to access restricted, unvetted, or age-restricted AI platforms on school grounds or devices is prohibited.

Reporting & Safeguarding

- **Data Breaches:** Any accidental input of personal data into an unvetted AI platform must be reported immediately to an SLT member.
- **Safeguarding Concerns:** Any inappropriate content, deepfakes, or harassment generated or received via AI must be reported directly to the Designated Safeguarding Lead (DSL).

Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

- Safer Internet Centre – <https://www.saferinternet.org.uk/>
- South West Grid for Learning – <https://swgfl.org.uk/products-services/online-safety/>
- Childnet – <http://www.childnet-int.org/>
- Professionals Online Safety Helpline – <http://www.saferinternet.org.uk/about/helpline>
- Revenge Porn Helpline – <https://revengepornhelpline.org.uk/>
- Internet Watch Foundation – <https://www.iwf.org.uk/>
- Report Harmful Content – <https://reportharmfulcontent.com/>

CEOP

- CEOP – <http://ceop.police.uk/>
- ThinkUKnow – <https://www.thinkuknow.co.uk/>

Others

- LGfL – Online Safety Resources – <https://www.lgfl.net/online-safety/resource-centre?a=3>
- Kent – Online Safety Resources page – <http://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials>
- INSAFE/Better Internet for Kids – <https://www.betterinternetforkids.eu/>
- UK Council for Internet Safety (UKCIS) – <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>
- Netsmartz – <http://www.netsmartz.org/>

Tools for Schools

- Online Safety BOOST – <https://boost.swgfl.org.uk/>
- 360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

- 360Data – online data protection self-review tool:
www.360data.org.uk
- SWGfL Test filtering - <http://testfiltering.com/>
- UKCIS Digital Resilience Framework -
<https://www.gov.uk/government/publications/digital-resilience-framework>
- Bullying/Online-bullying/Sexting/Sexual Harassment
- Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) -
<http://enable.eun.org/>
- SELMA – Hacking Hate - <https://selma.swgfl.co.uk>
- Scottish Anti-Bullying Service, Respectme -
<http://www.respectme.org.uk/>
- Scottish Government - Better relationships, better learning, better behaviour -
<http://www.scotland.gov.uk/Publications/2013/03/7388>
- DfE - Cyberbullying guidance -
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
- Childnet – Cyberbullying guidance and practical PSHE toolkit:
<http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit>
- Childnet – Project deSHAME – Online Sexual Harrassment -
<http://www.childnet.com/our-projects/project-deshame>
- UKSIC – Sexting Resources -
<https://www.saferinternet.org.uk/advice-centre/teachers-and-professionals/teaching-resources/sexting-resources>
- Anti-Bullying Network –
<http://www.antibullying.net/cyberbullying1.htm>
- Ditch the Label – Online Bullying Charity -
<https://www.ditchthelabel.org/>
- Diana Award – Anti-Bullying Campaign -
<http://www.antibullyingpro.com/>

Social Networking

- Digizen – Social Networking -
<http://digizen.org/socialnetworking/>

- UKSIC - Safety Features on Social Networks - <http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals/safety-features>
- Children's Commissioner, TES and Schillings – Young peoples' rights on social media - <https://www.tes.com/teaching-resources/digital-citizenship>

Curriculum

- SWGfL Evolve - <https://projectevolve.co.uk>
- UKCCIS – Education for a connected world framework - <https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis>
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources - <http://lreforschools.eun.org/web/guest/insafe>

Data Protection

- 360data - free questionnaire and data protection self review tool - <http://360data.org.uk/>
- ICO Guides for Education (wide range of sector specific guides) - <https://ico.org.uk/for-organisations/education/>
- DfE advice on Cloud software services and the Data Protection Act - <https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act>
- IRMS - Records Management Toolkit for Schools - https://c.ymcdn.com/sites/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf
- NHS - Caldicott Principles (information that must be released) - <https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx>
- ICO Guidance on taking photos in schools - <https://ico.org.uk/for-the-public/schools/photos/>
- Dotkumo - Best practice guide to using photos - <http://campuspr.co.uk/wp-content/uploads/2017/10/Commissioning-original-photography.pdf>

Professional Standards/Staff Training

- DfE – Keeping Children Safe in Education -
<https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>
- DfE – Safer Working Practice for Adults who Work with Children and Young People -
<http://www.safeguardingschools.co.uk/wp-content/uploads/2015/10/Guidance-for-Safer-Working-Practices-2015-final1.pdf>
- Childnet – School Pack for Online Safety Awareness -
<http://www.childnet.com/resources/school-pack-for-online-safety-awareness>
- UK Safer Internet Centre Professionals Online Safety Helpline -
<http://www.saferinternet.org.uk/helpline>

Infrastructure/Technical Support

- UKSIC – Appropriate Filtering and Monitoring -
<https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring>
- SWGfL Safety & Security Resources -
<https://swgfl.org.uk/resources/>
- Somerset – Questions for Technical Support -
<https://www.somerset.org.uk/sites/edtech/eSafety/Leading/Questions%20for%20Technical%20Support%202018.pdf>
- NCA – Guide to the Computer Misuse Act -
<https://nationalcrimeagency.gov.uk/who-we-are/publications/75-guide-to-the-computer-misuse-act/file>
- NEN – Advice and Guidance Notes -
<https://www.nen.gov.uk/advice/>

Working with parents and carers

- Online Safety BOOST Presentations – parent’s presentation -
<http://www.swgfl.org.uk/boost>
- Vodafone Digital Parents Magazine -
<http://www.vodafone.com/content/parents/digital-parenting.html>
- Childnet Webpages for Parents & Carers -
<http://www.childnet.com/parents-and-carers>

- Get Safe Online - resources for parents - http://www.getsafeonline.org/nqcontent.cfm?a_id=1182
- Teach Today - resources for parents workshops/education - <http://www.teachtoday.de/en/>
- Internet Matters - <https://www.internetmatters.org/>

Prevent

- Prevent Duty Guidance - <https://www.gov.uk/government/publications/prevent-duty-guidance>
- Prevent for schools – teaching resources - <http://www.preventforschools.org/>
- NCA – Cyber Prevent - <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved>
- Childnet – Trust Me - <https://www.childnet.com/resources/trust-me>

Research

- Ofcom –Media Literacy Research - <https://www.ofcom.org.uk/research-and-data/media-literacy-research>

Further links can be found at the end of the UKCIS Education for a Connected World Framework - <https://www.gov.uk/government/publications/education-for-a-connected-world>

Appendix 2

Rules for Responsible Internet Use

The school has installed computers with Internet access to help our learning. These rules will keep you safe and help us be fair to others.

- I will only access the system with my own login, which I will keep secret;
- I will not access other people's files;
- I will use the computers for school work and homework;
- I will not bring in pen drives from outside school
- I will ask permission from a member of staff before using the Internet;
- I will only Email people I know, or my teacher has approved;
- The messages I send will be polite and responsible;
- I will not give my home address or telephone number, or arrange to meet someone, unless my parent, carer or teacher has given permission;
- I will report any unpleasant material or messages sent to me. I understand this report would help protect other pupils and myself;
- I understand that the school may check my computer files and may monitor the Internet sites I visit.
- I will use the Google Workspace email system responsibly and any e-communications will only be about my school work.

Appendix 3

Responsible Use of the Internet Letter to Parents

Dear Parents

As part of pupil's curriculum enhancement and the development of ICT skills, Richard Avenue Primary School is providing supervised access to the Internet.

Pupils will be able to exchange electronic mail with partner schools and research information from museums, libraries, news providers and suitable web sites as part of their programme of learning.

We have our Internet access from the Local Education Authority that operates a filtering system that restricts access to inappropriate materials. All our screens are in public view and access will be supervised.

School issued Chromebooks are both filtered and monitored by the local authority, and only allow access to the internet between specific times.

The schools website contains information on internet safety, this is available for pupils and parents to access at home. Anyone wishing to know more about the dangers of the internet and what precautions they can take are invited to discuss their concerns with the ICT manager.

Yours Sincerely,
C Bolton