

Red Lane Primary School Online Safety Policy

Reviewed and Updated

September 2024 – L Healey

March 2025 – L Healey

Appendices & Policies that support this policy.

Appendix	
1	Online Safety Incident Flowchart
2	DFE Technical Standards for Bolton Schools
3	Acceptable User Agreements documents – Staff, Visitors & Volunteers
3.1- 3.4	Acceptable User Agreements documents –Pupils
4	Online Incident Report Log
5	School Safeguarding Policy
6	School Data Protection Policy
7	School 'AI' policy

Scope of the Policy

The regulation and use of technical solutions to safeguard children are important but must be balanced with teaching the necessary skills to enable pupils to take responsibility for their own safety in an ever-changing digital world. The National Computing Curriculum states that children should be able to use technology safely, respectfully, and responsibly keeping personal information private, recognise acceptable or unacceptable behaviour and identify a range of ways to report concerns about content and contact. Children's safety is paramount, and they will receive the help, guidance and support through the whole curriculum to enable them to recognise and avoid online risks and to build their resilience. During the delivery of the curriculum staff will reinforce and consolidate safe online learning

This policy applies to all members of the school community who have access to and are users of school ICT systems and online resources, both in and out of school.

The school will deal with incidents as outlined within this policy, within the remit of their safeguarding, behaviour and anti-bullying policies (and others when applicable).

Development of the Policy

This Online Safety Policy was approved by the Trustees on:	16 TH October 2023
--	-------------------------------

Schedule of Monitoring and Review

The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new Online threats or incidents that have taken place.	September 2025
The implementation of this Online Safety Policy will be monitored by the:	Headteacher Governors DSL Computing Lead / team
The school will monitor the impact of the policy using:	Identify children at greater risk of harm. Regular Audits of children and families' online behaviour and harms for baseline, this information to feed into risk assessment. Logs of reported incidents Monitoring logs of internet activity (including sites visited) Internal monitoring data for network activity
Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group at regular intervals:	Termly where appropriate
Should serious Online incidents take place, the following external persons / agencies should be informed:	Headteacher School DSL LADO Police See Appendix 1

KCSIE 2024

In line with KCSIE 2024, there is a stronger focus on filtering and monitoring in schools to ensure online safety. The guidance highlights that all staff members, including governors and trustees, must understand their roles and responsibilities in safeguarding children online. The Designated Safeguarding Lead (DSL) has explicit responsibility for overseeing online safety, including the implementation and regular review of the school's filtering and monitoring systems.

Schools are required to embed their approach to online safety, including appropriate filtering and monitoring, within their child protection policies. All staff should receive comprehensive safeguarding and child protection training (including online safety) during their induction, which must cover the expectations, roles, and responsibilities relating to filtering and monitoring. This training should be regularly updated—at least annually—and supplemented with ongoing updates through emails, e-bulletins, and staff meetings to ensure staff maintain the necessary skills and knowledge to safeguard children effectively.

The updated standards for filtering and monitoring now emphasise real-time content scanning and blocking illegal websites, reinforcing a secure digital environment for students. It is essential that the leadership team and relevant staff have a clear understanding of these systems to manage them effectively and address any concerns that arise.

Roles and Responsibilities

Headteacher:

The Headteacher has a duty of care for ensuring the day-to-day safety (including Online) of all members of the school community.

The role of the Headteacher will include:

- ensuring that all members of the school community understand and acknowledge their responsibilities in the event of a serious online allegation being made (**Appendix 1**)
- ensuring that all staff receive suitable **annual updates** for all staff members about their responsibilities regarding online safety, filtering, and monitoring and acknowledge and understand the potential for serious child protection / safeguarding issues.
- ensuring that the Online Safety Policy is accessible to the wider School Community (School website)
- meet at regular intervals with the DSL to ensure the implementation of this policy (as outlined above).
- ensuring the SLT receive regular monitoring reports from the DSL.
- ensuring there are opportunities to communicate up to date Online Safety information to the wider school community.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Anti-Bullying and Behaviour Policy.

Governors:

Governors are responsible for the approval of this Online Safety Policy and for reviewing its effectiveness. This will be carried out by the Governing board, receiving regular information about online incidents and monitoring reports.

The role of the Safeguarding Governor will include:

- regular meetings with the DSL
- regular monitoring of the Online Incident Log on CPOMS
- ensuring robust technical support is in place to keep systems safe and secure.
- regular monitoring of filtering
- reporting to the Governing board

- attending training for online safety where appropriate

Designated Safeguarding Lead (DSL)

DSL takes the lead role in managing online safety, ensuring that school has clear procedures to address any safeguarding concerns and uphold the school's prevent duty obligations.

The DSL will review and update the school's filtering and monitoring procedures, clearly defining roles and responsibilities within these processes. When assessing filtering and monitoring systems, governing bodies and SLT will consider the number of children at risk and the proportionality of costs versus safety risks.

The DSL will evaluate the strength and suitability of the current cyber security measures and consider improvements where necessary.

The DSL will ensure that the school's Safeguarding policy adequately reflects its approach to online safety, including appropriate filtering and monitoring on school devices and school networks.

The DSL is responsible for taking any necessary action as per the Online Safety Incident reporting flowchart (**Appendix 1**).

They will arrange regular training and provide **annual updates** for all staff members about their responsibilities regarding online safety, filtering, and monitoring and acknowledge and understand the potential for serious child protection / safeguarding issues that arise from, but not limited to

- sharing of personal data
- accessing illegal / inappropriate materials
- exposure to inappropriate online content
- inappropriate contact with adults/strangers
- potential or actual incidents of grooming
- sexting
- cyber-bullying

In the event of a child protection or safeguarding incident pertaining to the above, the DSL will refer to **appendix 1**.

Computing Lead / Team

The Computing Lead has the responsible for the teaching and learning of online safety across the whole school. The school has raised the profile of online safety and has expanded the computing curriculum to include a fourth strand of Digital Citizenship, the Education for a Connected World framework is used to support the teaching of Digital Citizenship and PHSE across all year groups.

The role of the Computing Lead/team includes:

- providing advice for staff and signpost relevant training and resources
- liaising with relevant outside agencies
- liaising with relevant technical support teams
- as needed to support DSL reviewing reports of Online Incidents (**CPOMS**)
- meeting regularly with Headteacher to discuss issues and subsequent actions.
- acting in response to issues identified
- communicating up-to-date Online Safety information to the wider school community

School Staff

It is essential that all staff.

- receive **annual** appropriate safeguarding and child protection training, including online safety which, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- understand and acknowledge their responsibilities as outlined in this Policy.
- have read, understood and signed the Staff Acceptable Use Policy (Appendix 3)
- keep up to date with the Online Safety Policy as part of their CPD.

- will not support or promote extremist organisations, messages, or individuals.
- will not give a voice or opportunity to extremist visitors with extremist views.
- will not browse, download, or send material that is considered offensive or of an extremist nature by the school.
- have an up-to-date awareness of online matters pertinent to the children that they teach/have contact with
- report concerns and log incidents. (CPOMS)
- ensure that all digital communications with the School Community are on a professional level and only carried out using official school approved systems.
- apply this Online Safety Policy to all aspects of the Curriculum.
- share, discuss and ensure the children understand and acknowledge their responsibility to follow their age-appropriate Acceptable Use Agreements.
- are good role models in their use of all digital technologies.
- are vigilant in monitoring how pupils use digital technologies and access online content whilst in their care.

It is accepted that from time to time, for purposeful/appropriate educational reasons, pupils may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so should be auditable with clear reasons for the need.

Technical support

The school's technical infrastructure must be secure and actively reduces the risk of misuse or malicious attack. To facilitate this, school has purchased support from Bolton Schools ICT.

The role includes:

- Follow the [DFE digital and technology standards in schools](#)
- provide a secure Wi-Fi system for both staff and guests with in your setting
- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems
- procure systems (with SLT &DSL)
- identify risk (with SLT &DSL)
- carry out reviews (with SLT &DSL)
- carry out checks (with SLT & DSL)
- ensuring that detected risks and/or misuse is reported to the Headteacher at school.
- ensuring that schools are informed of any changes to guidance or any planned maintenance.
- school technical systems will be managed and reviewed annually in ways that ensure that the school meets recommended technical requirements.
- all users will have clearly defined access rights to school technical systems and devices.
- all school network users will be assigned an individual username and password at the appropriate level of access needed for their role.
- ensuring internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the [Internet Watch Foundation](#) Child Abuse Image Content list (CAIC).
- content lists are regularly updated, and internet use is logged and regularly monitored.
- there is a clear process in place to deal with requests for filtering changes.
- provide a platform where school should report any content accessible in school but deemed inappropriate.
- ensuring appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software (**Appendix 2**)

Pupils

The children's learning will progress through a broad, effective and relevant Online Safety curriculum.

A pupil's learning journey will be holistic in that it will include, but is not limited to their online reputation, online bullying and their health and wellbeing.

It is essential that all pupils should:

- understand, acknowledge and adhere to their age-appropriate Acceptable Use Policy (**Appendix 3**)
- be able to recognise when something makes them feel uncomfortable (butterfly feeling) and know how to report it.
- accept their responsibility to respond accordingly to any content they consider as inappropriate.
- understand the importance of being a responsible digital citizen and realise that the school's Online Safety Policy applies to their actions both in and out of school.
- know that school will act in response to any breach of the Online Safety Policy

Parents / Carers / Responsible adults

Parents play an essential role in the education of their children and in the monitoring / regulation of the children's on-line usage. Due to the ever-evolving Digital World, adults can sometimes be unsure of how to respond to online risks and issues. They may also underestimate how often pupils encounter potentially harmful and inappropriate online material.

Therefore, it is essential that all adults should:

- promote safe and responsible online practice and must support the school by adhering to the school's Safeguarding and Online Safety Policy in relation to digital and video images taken whilst on school premises or at school events.
- understand, acknowledge their child's Acceptable Use Policy (**Appendix 3.1-4**)
- understand and ensure that they and their child adhere to school procedure relating to their use (or prohibition) of personal devices whilst on school grounds.

To support the school community, school will provide information and awareness through, but not limited to:

- letters, newsletters, website links, publications, external agencies
- Parents / Carer workshops
- high profile events / campaigns e.g. Safer Internet Day

Visitors entering school

It is essential that school apprise visitors of all relevant policies pertaining to their visit and contact with pupils.

Useful Information

Safeguarding

In the event of a Safeguarding infringement or suspicion, **appendix 1** must be followed with consideration of the following:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a computer that will not be used by pupils and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the investigation, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
- Record any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and signed (except in the case of images of child sexual abuse – see below)
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include incidents of 'grooming' behaviour the sending of obscene materials to a child adult material which potentially breaches the Obscene Publications Act criminally racist material other criminal conduct, activity or materials. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the school for evidence and reference purposes.

Data Protection

Personal and sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. Schools are audited regularly regarding how they handle their data, for further information please refer to school Data Protection Policy (**Appendix 5**).

Communications

When using communication technologies the school considers the following as good practice:


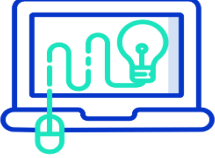

- The Office 365 school email service is safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school.
- When accessing emails out of the schools setting, staff will only be able to access their schools' emails using Microsoft Multifactor Authentication app.
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents / carers (email, chat) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about online issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media


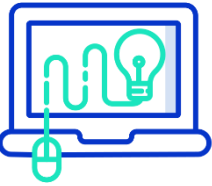


The school's use of social media is to promote the ethos of the school. It is the responsibility of all staff to ensure that the content they upload is for professional purposes only, be compliant with the school policies and protect the identity of pupils.

 <p>NCA Young people can report concerns about child sexual abuse and exploitation to NCA</p>	 <p>Report Remove A free tool that allows children to report nude or sexual images and videos of themselves that they think might have been shared online</p>	 <p>ChildLine A free, private and confidential service where CYP can talk about anything to a trained counsellor, online or on the phone</p>	 <p>NSPCC Report Abuse in Education The Report Abuse in Education helpline offers support and guidance to CYP and who have experienced or witnesses sexual harassment or abuse in schools</p>
---	---	---	---





Year 1 and Year 2 Technology Agreement

 <p>My Learning</p> <p>Using technology @school</p> 	<p>My conduct as a Digital Citizen</p> <ul style="list-style-type: none"> • I will be respectful when I use a school device (PCs, laptops, tablets/ ipads) for my learning and tell a teacher if I am struggling or something is not working properly. I won't use my own device at school. • I know I need to follow our online safety rules to help me keep safe and healthy online at school when using technology. • I will only use activities that my teacher has told or allowed me to use. • I will be kind online, so I do not upset my friends. • I can talk about my digital footprint and will use what I have learned about Online Safety in school to search safety. • I will tell my teacher if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.
 <p>Using technology @home</p>	<p>My online world content</p> <ul style="list-style-type: none"> • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I may be putting myself at risk of cyberbullying. • I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen. <p>My online world contact</p> <ul style="list-style-type: none"> • Where I have my own username and password, I will keep it safe and secret. • I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details) • I will tell a trusted adult if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.

Year 3 and Year 4 Technology Agreement

 <p>My Learning</p>	<ul style="list-style-type: none"> • I will be respectful when I use a school device (PCs, laptops, tablets/ ipads) for my learning and tell a teacher if something is not working properly or I am struggling. <p>My School Accounts</p> <ul style="list-style-type: none"> • I will keep my usernames and passwords safe and secure - I will not share them. • I will not use anyone else's username and password. • I will only use apps, programs, or websites that my teacher has told me to use. • I will save only schoolwork on the school network.
 <p>Using technology @school</p>	<p>My conduct as a Digital Citizen</p> <ul style="list-style-type: none"> • I know that I can talk to my teachers about my digital footprint and if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen, I can tell them. • I will respect other people's work and property and will not access, copy, delete any other user's files. • I know that I should check the content on websites as not everything is real or true. • I will not use personal devices, such as cameras, watches or phones at school
 <p>Using technology @home</p> 	<p>My online world content</p> <ul style="list-style-type: none"> • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I may be putting myself at risk of accessing inappropriate content and cyberbullying. • I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen. <p>My online world contact</p> <ul style="list-style-type: none"> • I will be aware that new friends made online may not be who they say there. • I will be aware of what information cannot be shared between my friends. • I will be polite and responsible when I communicate with others online. • I will not use inappropriate language and I understand that others may have different opinions than me. <p>My online world conduct</p> <ul style="list-style-type: none"> • I understand that spending too much time online is not always good for me. • I understand that content I share online can still be there even after I have deleted it. • I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen. • With the help of a trusted adult I will report any inappropriate content, messages or anything that makes me feel uncomfortable online, using the app/social media reporting tool or other online support agencies e.g. CEOP, Childline, Barnardos.

Year 5 and Year 6 Technology Agreement

 <p>My Learning</p>	<ul style="list-style-type: none"> • I will be respectful when I use a school device (PCs, laptops, tablets/ipads) for my learning and tell a teacher if something is not working properly or I am struggling. <p>My School Accounts</p> <ul style="list-style-type: none"> • I will keep my usernames and passwords safe and secure - I will not share them. • I will not use anyone else's username and password. • I will only use apps, programs, or websites that my teacher has told me to use. • I will log off or shut down a computer when I have finished using it.
 <p>Using technology @school</p>	<p>My conduct as a Digital Citizen</p> <ul style="list-style-type: none"> • I know that I can talk to my teachers about my digital footprint and can report any unpleasant or inappropriate content, messages or anything that makes me feel uncomfortable when I see it online to a trusted adult. • I know that some websites may present 'opinions' as 'facts'; whilst the popularity of an opinion or the personalities of those promoting it does not necessarily make it true, fair or perhaps even legal. • I will respect other people's work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission. • I will not take or distribute images or voice recordings of anyone without their permission.
 <p>Using technology @home</p> 	<p>My online world content</p> <ul style="list-style-type: none"> • I understand that certain sites and games have age restrictions to keep me safe. • I understand that by accessing such sites and games, I may be putting myself at risk of accessing inappropriate content and cyberbullying. • I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen. <p>My online world contact</p> <ul style="list-style-type: none"> • I will be aware that new friends made online may not be who they say there. • I will be aware of what information cannot be shared between my friends. • I will be aware of regularly checking privacy on apps to keep me safe. • If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me. <p>My online world conduct</p> <ul style="list-style-type: none"> • I understand that spending too much time online is not always good for me. • I will be polite and responsible when I communicate with others online. • I will not use inappropriate language and I understand that others may have different opinions than me. • I understand that content I share online can still be there even after I have deleted it. <p>My online world commerce</p> <ul style="list-style-type: none"> • I understand that there are some sites that have a high risk of me accessing content such as online gambling, inappropriate advertising, phishing and or financial scams.

- | | |
|--|---|
| | <ul style="list-style-type: none">• With the help of a trusted adult I will report any inappropriate content, messages or anything that makes me feel uncomfortable online, using the app/social media reporting tool or other online support agencies e.g. CEOP, Childline, Barnardos. |
|--|---|