Prestolee Primary School Online Safety Policy

Reviewed and Updated

5th February 2025

Appendices & Policies that support this policy.

Appendix	
	Online Safety Incident Flowchart
	DFE Technical Standards for Bolton Schools
	Acceptable User Agreements documents – Staff, Visitors & Volunteers
	Acceptable User Agreements documents –Pupils
	Online Incident Report Log
	School Safeguarding Policy – Schools Own
	School Data Protection Policy – Prestolee Multi Academy Trust Own
	School 'AI' policy – sample emailed to schools

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-bulling policies (and others when applicable).

Development of the Policy

This Online Safety Policy has been developed by Bolton Schools ICT. It is recommended that this Policy is reviewed and ratified by the school's own relevant parties* i.e.

- Headteacher
- Governing Body
- Designated Safeguarding lead (DSL)
- Computing lead / team

This Online Safety Policy was approved by the Governing Body *on:*	May 2025

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.	5th February 2026
The implementation of this Online Safety Policy will be monitored by the:	Headteacher Governors DSL has responsibility for online safety, to then liaise with relevant parties to develop action plan. Computing Lead
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. Online Safety Risk Assessment- 360 template. 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, within linked Governor meetings on Safeguarding.

* In this policy whenever the term 'relevant parties' is used, school need to nominate who is responsible from this list

Should serious Online incidents take place, the following external persons / agencies should be informed:	Headteacher School DSL LADO Police **See Appendix 1**

Digital Resilience:

The internet has become part of our everyday lives and is now easier to access than ever before, but using the internet can also have risks. Children and young people are more at risk of exposure to inappropriate or criminal behaviour if they are unaware of the dangers.
Digital Resilience is a term given to 'the social and emotional literacy and digital competency to positively respond to and deal with any risks they (pupils) might be exposed to when they are using social media or going online'.
Being digitally resilient is about being able to deal with any incidents that go awry online especially on social media.
We aim to equip our pupils with the emotional resources needed to understand when they might be at risk online.

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 relevant parties 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.

Where appointed, the role of the Online Governor will include:

- regular meetings with the DSL
- regular monitoring of the Online Incident Log/CPOMS** (which will include anonymous details of Online Incidents Report Log)
- 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

** If a school is using CPOMS it is important to ensure that the lozenges are set up to be specific and appropriate, for example – PEGI, Tik Tok, Snapchat, Instagram etc. This will assist in collating and responding to Online Incidents.

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 relevant parties 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/ child protection 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
- 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.
- keep up to date with the Online Safety Policy as part of their CPD.
- will not support or promote extremist & terrorist 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.

- 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 Technology 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.

Researching Sensitive Topics

It is understood that, for educational purposes, pupils may occasionally need to research sensitive or challenging topics, such as racism, drugs, or discrimination. In such cases, this may trigger a Safeguarding alert, which will include details of the content that was searched.

The Designated Safeguarding Lead (DSL) will review the alert and investigate the situation further, ensuring that appropriate steps are taken to support the pupil and address any potential concerns.

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, or school has support from…
The role includes:

- Follow the DFE digital and technology standards in schools
- provide a secure Wi-Fi system – current set up with a designated school Wi-Fi for school device access and separate Wi-Fi for non-school devices and guest users.
- maintaining filtering and monitoring systems
- providing filtering and monitoring alerts
- completing actions following concerns or checks to systems.
- procure systems (with SLT, Governors & DSL)
- identify risk (with SLT, Governors & DSL)
- carry out reviews (with SLT, Governors & DSL)
- carry out checks (with SLT & DSL)
- ensuring that monitoring alerts are reported to the DSL and nominated staff at school via a specific Safeguarding email
- 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.

Pupils and Online Safety

Pupils will progress through a comprehensive, effective, and relevant Online Safety curriculum, which is designed to support their overall learning journey. This journey will be holistic, covering not only their academic development but also areas such as their online reputation, online bullying, and overall health and well-being.

It is essential that all pupils:

- Pupils must acknowledge and follow their age-appropriate Technology Agreement (Acceptable Use Policy), which sets clear expectations for their online behaviour.
- Pupils should be able to identify when something online makes them feel uncomfortable (often referred to as the "butterfly feeling") and know how to report it appropriately.
- Pupils must accept responsibility for responding appropriately to any content they encounter that they consider inappropriate.
- Pupils should understand the importance of being responsible digital citizens, recognizing that the school's Online Safety Policy applies to their behaviour both in and outside of school.
- Pupils should be aware that the school will act in response to any breach of the Online Safety Policy.

By following these guidelines, pupils can ensure that they are equipped to navigate the online world safely, responsibly, and with respect for themselves and others.

Parents / Carers / Responsible adults

Parents and carers play a crucial role in their children's education and in overseeing their online activities. As the digital world continues to evolve, it is understandable that adults may sometimes feel uncertain about how to address online risks and issues. Additionally, they may not fully realize how frequently children encounter potentially harmful or inappropriate online material.

To support the safety and well-being of all students, it is essential that all adults take the following steps:

- Adults must encourage safe and responsible online behaviour. They should support the school by adhering to the school's Safeguarding and Online Safety Policy, especially regarding the taking and sharing of digital and video images during school activities and events.
- Parents and carers should ensure they understand and acknowledge their child's Technology Agreement (Acceptable Use Policy), which outlines the expectations for online behaviour.
- Adults should understand and acknowledge that their child follows the school's procedures for the use of personal devices on school grounds.

To assist parents and carers in supporting their child's online safety, the school will provide information and resources through various channels, including:

- Letters, newsletters, website links, publications, and external agencies
- Parents/carers workshops
- High-profile events and campaigns, such as Safer Internet Day

By working together, the school and parents can help children navigate the online world safely and responsibly.

Visitors entering our school.

It is important for the school to inform visitors of all relevant policies regarding their visit and interaction with pupils. This ensures a safe and secure environment for everyone.

- All visitors must be made aware of the school's policies that relate to their visit and any interactions they may have with students. This includes safeguarding, behaviour, and confidentiality policies.
- Visitors who require access to the Guest WiFi network should be informed that the content accessed on their personal devices is monitored by the school's IT systems. This monitoring is in place to ensure the safety and security of the network and its users.

Social Media Usage Guidelines for Staff

Our school uses social media as a tool to promote its ethos and values. When sharing content, staff must ensure that they adhere to the following guidelines:

- Staff should take extra care to avoid sharing any personal information about pupils. Content must not identify or disclose details about students without explicit consent.
- All social media content uploaded by staff should be for professional purposes only. Staff must ensure that posts align with the school's mission, values, and policies.
- It is the responsibility of all staff to ensure that the content they upload is fully compliant with school policies, especially those concerning safeguarding and confidentiality.
- Staff must take necessary precautions to protect the identity of pupils. Any images or content shared should not compromise the privacy of students.

Useful Information

Safeguarding

In the KCSIE 2023 there is a greater emphasis on filtering and monitoring in schools. The document stresses the importance of all staff members understanding their duties and obligations regarding online safety. Schools are advised to reflect their approach to online safety, including appropriate filtering and monitoring on school devices and networks, in their child protection policy.
'All staff should receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – see para 141 for further information) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.' * DFE - KCSIE 2023

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 Office 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**. Personal data MUST NOT be stored on any portable computer or memory stick or any other removable media. All teachers have been issued with remote access on school laptops to ensure that when access data at home can only be done by using two factor authentication, staff to be mindful of not leaving their work device unattended.

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.