Heathfield Primary School

ONLINE SAFETY POLICY

Our Mission Statement:
Learning together, Learning for Life

Chair of Governors	Sharmeen Atcha
Headteacher	Mark Thornley
Policy written by	BOLTON ICT / Heathfield
Date approved by governors	September 2025

Documents that support this policy:

APPENDIX

1 Online Safety Incident Flowchart

2 DFE Technical Standards for Bolton Schools

OTHER RELATED POLICIES:

Acceptable User Agreements– Staff, Visitors & Volunteers

Guest WIFI Notice

Safeguarding Policy

Data Protection Policy

'AI' policy

SCOPE OF THE POLICY

The regulation and use of technical solutions to protect children online are crucial, but they must be balanced with the responsibility to teach pupils the skills necessary to safeguard themselves in an ever-evolving digital environment. It's essential that, alongside technical protections like firewalls, monitoring and filtering, children are equipped with the knowledge and confidence to make safe and informed decisions while using technology. The National Computing Curriculum emphasises the need for children to use technology in a safe, respectful and responsible manner. This includes:

- Keeping personal information private, ensuring that children understand the importance of privacy and the risks of oversharing online.
- Recognising acceptable and unacceptable behaviour online, such as distinguishing between respectful communication and harmful actions like cyberbullying or harassment.
- Identifying multiple ways to report concerns about inappropriate content or online interactions, empowering children to seek help when needed.

In line with these goals, schools have a duty to ensure that children are equipped with the knowledge and skills to recognise online risks. Through the curriculum, pupils will receive continuous help, guidance and support that:

- Teaches them how to recognise and avoid online dangers such as cyberbullying, inappropriate content and online predators.
- Helps them build resilience so they can respond positively to online challenges and recover from negative experiences.
- Reinforces safe online learning practices through repeated exposure and integration across various subjects, promoting good digital citizenship.

This policy applies to everyone in the school community who uses school ICT systems and online resources, both during school hours and beyond. This means that staff, pupils and any other users of school technology are all expected to adhere to these standards of safe, responsible use.

In the event of an online incident, the school will follow a set protocol as outlined in the policy. This includes addressing incidents within the framework of existing safeguarding, behaviour and anti-bullying policies, ensuring that appropriate measures are taken in response to any concerns. By integrating online safety into the curriculum and having clear procedures in place for handling incidents, the school aims to create a safe and supportive digital environment for all its pupils.

DEVELOPMENT OF THE POLICY

This Online Safety Policy has been developed by Bolton Schools ICT.

This Online Safety Policy was approved by the Governing Body in February 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.

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.

The school will monitor the impact of the policy using:

- Identify children at greater risk of harm.
- Complete an audit of children and families' online behaviour and harms for baseline, this information to feed into risk assessment.
- Complete the 175 Safeguarding Audit 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 termly report on the implementation of the Online Safety Policy

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

DIGITAL RESILIENCE:

Digital Resilience is essential in today's connected world, where the internet plays a significant role in the lives of children and young people. With the increasing use of digital platforms for socialising, learning and entertainment, it's crucial that young people are aware of the potential dangers they could face online.

The concept of Digital Resilience emphasises the development of both social-emotional skills and digital competencies that help individuals recognise, avoid and respond to risks. These might include cyberbullying, exposure to inappropriate content or misinformation. Being digitally resilient means that children and young people not only know how to identify and avoid these risks but also understand how to handle situations when they do occur.

To equip young people with the tools to navigate these online challenges:

- Children need to be taught about the potential dangers of the digital world, such as privacy concerns, the importance of safe online behaviour and how to report harmful content.

- Developing emotional intelligence and coping strategies helps young people stay calm, confident and proactive when faced with online challenges. This includes encouraging open discussions about online experiences and emotions.

- By encouraging critical thinking and digital literacy, we empower our pupils to make informed decisions online, handle conflicts and know what actions to take if they encounter something troubling.

- Creating a safe space where children feel comfortable talking about their online experiences with trusted adults helps reinforce their resilience. Encouraging regular conversations about their digital lives can increase their confidence in navigating the online world.

Ultimately, Digital Resilience is not just about preventing negative experiences but also about building the confidence and ability to recover and learn from mistakes or challenges encountered 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 governors 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 cyberbullying 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/ Computing lead/team.
- 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.

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 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 and 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 (Appendix1).

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 AND CURRICULUM LEAD

The Computing Lead is 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 PSHCE 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.

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, recognising 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.

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

The role includes:

- follow the DFE digital and technology standards in schools.
- 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).
- provide and maintain filtering and monitoring solutions in line with recommended standards.
- provide a platform where school should report any content accessible in school but deemed inappropriate.
- there is a clear process in place to deal with requests for filtering changes.
- provide a solution which enables DSLs and nominated staff to receive alerts by having access to a specific Safeguarding email.
- ensuring appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date virus software. These are tested regularly.
- school technical systems will be managed and reviewed annually in ways that ensure that the school meets recommended technical requirements, ensuring that schools are informed of any changes to guidance or any planned maintenance.
- 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.
- 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.
- completing actions following concerns or checks to systems.
- procure systems (with SLT, Governors & DSL).
- identify risks and where needed carry out and support reviews and checks (with SLT, Governors & DSL).

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 realise how frequently children encounter potentially harmful or inappropriate online material.

To support the safety and well-being of all pupils, 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 (AUPs), 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 pupils. 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 pupils 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 statement, 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 pupils.

USEFUL INFORMATION

Safeguarding

The Keeping Children Safe in Education guidance emphasises the critical role that filtering and monitoring play in ensuring online safety within schools. The document stresses that schools must have strong systems in place to manage the use of technology and all staff members must understand their responsibilities regarding online safety. This includes having clear policies for filtering and monitoring both school devices and networks to protect students from harmful or inappropriate content.

Filtering and Monitoring:

- Schools are expected to ensure appropriate filtering and monitoring mechanisms are in place on devices and networks that pupils use. This helps prevent access to harmful material and allows schools to monitor activity to protect students from risks like cyberbullying, exposure to inappropriate content and online predators.

- It is vital for the school's Online safety policy to reflect the approach to filtering and monitoring, ensuring it is embedded within the broader safeguarding framework.

Staff Responsibilities:

- All school staff regardless of their specific role, must understand their duties related to online safety, including the expectations and responsibilities associated with filtering and monitoring. They should be aware of what steps to take if they notice any concerning online behaviour or content.

- ·The guidance stresses the importance of training all staff members on safeguarding and child protection, including online safety, right from their induction. This ensures that everyone is equipped with the knowledge and skills to safeguard students effectively.

- This training should be regularly updated and schools should ensure that all staff receive ongoing safeguarding and online safety updates throughout the year, such as through email, e-bulletins or staff meetings. At least annual updates are necessary to ensure that staff are kept up-to-date with the latest developments, risks and best practices in safeguarding and online safety.

The Importance of Online Safety Training:

- The inclusion of online safety within safeguarding training ensures that staff are not only able to recognise and respond to traditional safeguarding concerns but also are equipped to handle online threats. This proactive approach helps create a safer environment for pupils in both physical and digital spaces.

- By regularly updating and reinforcing staff training, schools create a culture of vigilance and responsiveness to the rapidly changing landscape of online risks and threats.

The KCSIE 2 guidance highlights the importance of a proactive and comprehensive approach to online safety within schools. This includes ensuring that appropriate filtering and monitoring mechanisms are in place to protect pupils, while also ensuring that staff are continuously educated and equipped to handle safeguarding issues in the digital age. By integrating these practices into the school's safeguarding policies and training programs, schools can provide a safer online environment for students.

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 access to remote access through two factor authentications, which must be used and 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.