St Mary's RC Primary School
Online Safety Policy

Reviewed and Updated

September 2025

Documents that support this policy.

Appendix	
1	Online Safety Incident Flowchart
	Online Incident Report Log
	DFE Technical Standards for Bolton Schools
	Acceptable User Agreements– Staff, Visitors & Volunteers
	Technology Agreements – Pupils
	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. 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:*	November 2025

Schedule of Monitoring and Review

The Online Safety Policy will be reviewed annually or more regularly in the light of any	September 25

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

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

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.
- ensure a structured and responsible approach to **AI** implementation in the school, designated school leaders (see below) should be assigned to oversee this integration.
- 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.

Headteacher and Senior Leaders
The headteacher and senior leaders (including those within the AI Leadership Team – referenced in the AI Policy) are responsible for the strategic planning of how AI will be used in the school, establishing AI policies and procedures and ensuring that all staff receive relevant training and have a clear understanding of these.

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 Safety/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.
- has a good understanding of how **AI** is used in a school context and potential benefits and risks of its use.
- 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 (**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**.

Designated Safeguarding Lead / Online Safety Lead

Our Designated Safeguarding Person and Online Safety Lead have responsibility for online safety in the school. They are expected to have knowledge of **AI** and its safeguarding implications and an in-depth working knowledge of key guidance. We ensure that they receive appropriate specialist training, commensurate with their role and that ongoing training is provided for all school staff.

Computing Lead / Team

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 and relevant parties 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.
- must report any incidents or suspected incidents concerning the use of **AI** in line with school policy.
- when using **AI** staff will challenge any inappropriate behaviour.
- 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) are able to review any alerts and investigate the situation further, ensuring that appropriate steps are taken to support the pupil and address any potential concerns. When an email alert is received staff can view the alert in the Lightspeed portal by clicking on the **blue button** labelled **'View Alert'**, this will take you to the Lightspeed login page https://login.lightspeedsystems.app.

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).
- 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.
- 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.
- 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).
- 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. it is good practice to notify Bolton Schools ICT of any staff or pupils that have left so we can disable their accounts.

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 been issued with two factor authenticator apps software to ensure that when accessing data at home two factor authentication 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:

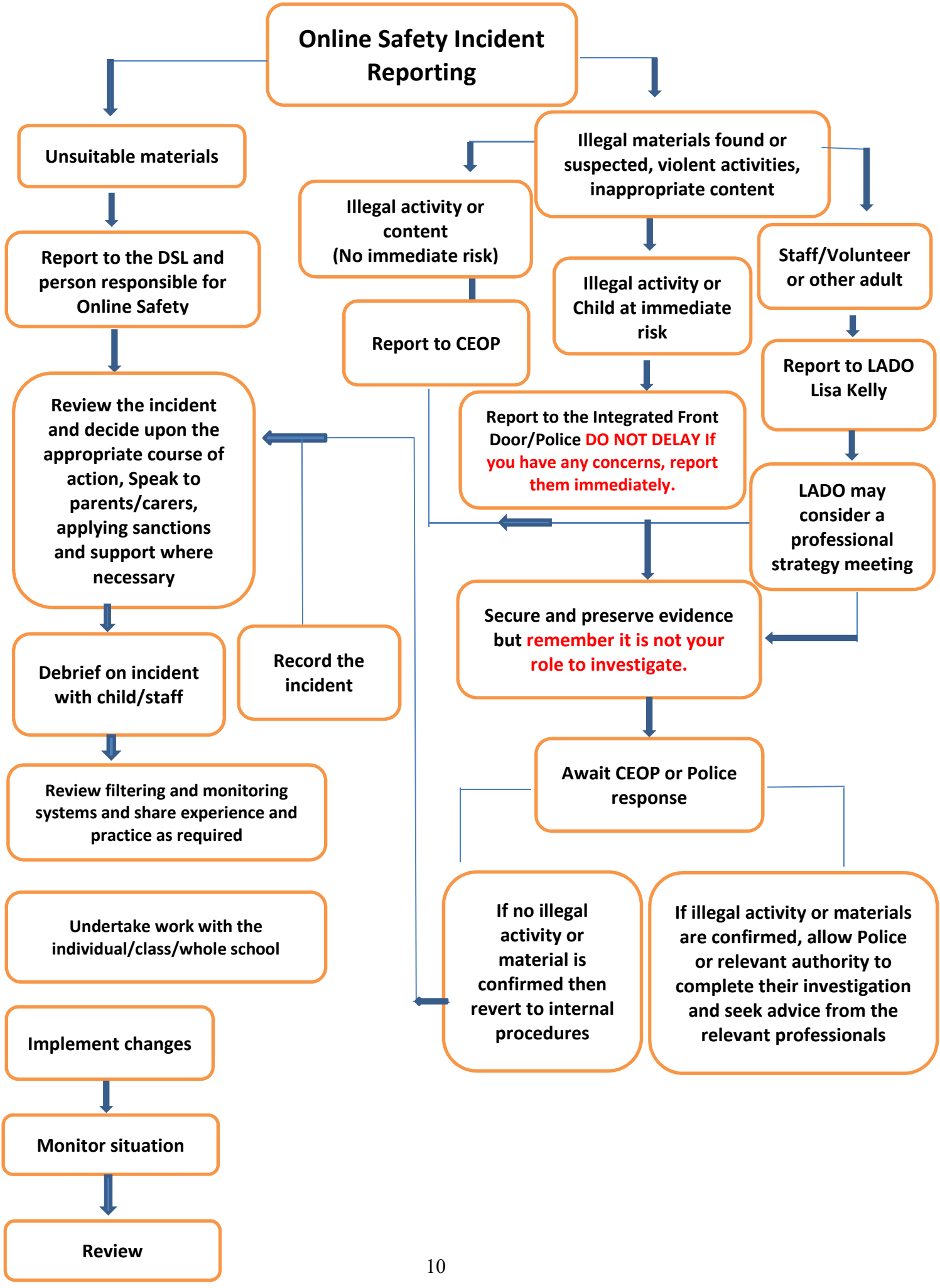
- The Office 365 school email service is safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school.
- When accessing emails out of the schools setting, 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.

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.



Appendix 1


Online Safety Incident Reporting
Unsuitable materials
Report to the DSL and person responsible for Online Safety
Review the incident and decide upon the appropriate course of action, Speak to parents/carers, applying sanctions and support where necessary
Debrief on incident with child/staff
Review filtering and monitoring systems and share experience and practice as required
Undertake work with the individual/class/whole school
Implement changes
Monitor situation
Review
Record the incident
Illegal activity or content (No immediate risk)
Report to CEOP
Illegal materials found or suspected, violent activities, inappropriate content
Illegal activity or Child at immediate risk
Report to the Integrated Front Door/Police DO NOT DELAY If you have any concerns, report them immediately.
Staff/Volunteer or other adult
Report to LADO Lisa Kelly
LADO may consider a professional strategy meeting
Secure and preserve evidence but remember it is not your role to investigate.
Await CEOP or Police response
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professionals

Support for Bolton Schools

SET – Safeguarding in Education Team:

- Jo Nicholson– Safeguarding in Education Officer – 07917072223
- Natalie Mckeon– Safeguarding Education Social Worker – 07384234744
- SET@Bolton.gov.uk

LADO: Lisa Kelly- 07824541233

Integrated Front Door – 01204 331500

Police protection investigation unit – 0161 856 7949

Community Police - 101

Complex Safeguarding Team – Exitteam@bolton.gov.uk

If there is an ICT network issue, contact your school ICT provider.

If your provider is Bolton School ICT Unit – contact 01024 332034 or contact@sict.bolton.gov.uk

Next steps

- Consider if an individual safety plan is required.
- Consider opening an early help assessment
- Ensure that data inputting procedures are in place and that data is shared with relevant governance.

Appendix 2 St Mary's RC Primary School

Staff, Visitors and Volunteers Acceptable Use Policy

Innovative technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational and personal use.
- that school / academy IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of IT in their everyday work.

The school will ensure that staff and volunteers will have good access to IT to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use the school IT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the IT systems and other users. I recognise the value of the use of technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of IT. I will, educate the young people in my care in the safe use of technology and be a good role model in my own use of all digital technologies in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the IT systems, email and other digital communications;
- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school;
- I will not support or promote extremist organisations, messages, or individuals;
- I will not give a voice or opportunity to extremist visitors with extremist views;
- I will not browse, download, or send material that is considered offensive or of an extremist nature by the school;
- I understand that the school IT systems are intended for educational use;
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

Staff passwords:

- **All staff users will be provided with a username and password** by *Bolton Schools ICT who will keep an up to date record of users and their usernames.*
- ***A password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters and must not include proper names or any other personal information*** about the user that might be known by others.
- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of to the DSL.
- I will be professional in my communications and actions when using school / academy IT systems.

- I will not access, copy, remove or otherwise alter any other user's files, without their expressed permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images.
- I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website /social media platforms) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school/academy:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school / academy IT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will ensure that my data is regularly backed up, in accordance with relevant school / academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose, or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). **Where digital personal data is transferred outside the secure local network, it must be encrypted.** Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work;
- where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*:

I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school / academy IT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school/academy.

St Mary's RC Primary School

Staff, Visitors and Volunteers Acceptable Use Policy

I understand that if I fail to comply with this Acceptable Use Policy, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the Police.

I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when conducting communications related to the school) within these guidelines.

Staff/Visitor/Volunteer Name	
Signed	
Date	

Appendix 3 Example of EYFS Technology Agreement

<table>
<tr>
<td>

My Learning

Using technology @school

</td>
<td>My conduct as a Digital Citizen

• 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.
• I will ask a teacher before using a device and ask for help if I can’t work the device.
• I will only use activities that a teacher has told me to use.
• I will ask a teacher if I am not sure what to do or think I have done something wrong.
• I can talk about my digital footprint and will try to use what I have learned about Online Safety in school.
• I know that there are rules that I need to follow to help me keep safe and healthy online at school when using technology.
• I will only use the internet when the teacher says I can.
• I will tell my teacher if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.
</td>
</tr>
<tr>
<td>

Using technology @home</td>
<td>My online world content

• I know that there are rules that I need to follow to help me keep safe and healthy online at home when using technology.
• I will tell a trusted adult if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.</td>
</tr>
</table>

Notes for School

Good Practice

At the beginning of a term, to review as part of a lesson when using technology.
To have a A3 class agreement on display so it can be referred during lessons where technology is being used.

This paragraph can be included when sending online safety updates home.

Parents / Carers:

Please encourage your child/children to adopt safe use of the internet and their devices at home.

Throughout the year your child/children will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

The school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and IT systems. The school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

If you have any concerns over your child/children's online safety experience do not hesitate to contact school for advice.

Appendix4

ONLINE INCIDENT LOG

Details of ALL Online incidents to be recorded by the staff within your School, this incident log will be monitored weekly by the DSL.

Date & time	Name of child or staff member	Male or Female	Room and computer/ device number	Details of incident (including evidence)	Actions and reasons