



At Claypool everyone is valued, inspired and nurtured on their individual journey of success.

Online Safety Policy

Policy lead: B. Matthews

Last interim review by the Policy Lead	Autumn 2025
Last full review by the Policies Committee	Autumn 2025

Next interim review by the Policy Lead	Autumn 2026
Next full review by the Policies Committee	Autumn 2026

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 has been developed by a working party led by Bolton Schools' ICT. This Policy is monitored, reviewed and ratified by the following:

Head teacher – Amanda Hulme

Board of Governors

Safeguarding lead – Amanda Hulme

Computing lead – B Matthews

Roles and Responsibilities

Head teacher

The Head teacher 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 Head teacher 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 relevant staff receive suitable training to enable them to carry out their safeguarding responsibilities within the remit of the Online Safety Policy
- ensuring that the Online Safety Policy is accessible to the wider School Community (School website)
- meeting at regular intervals with the Computing Lead to ensure the implementation of this policy (as outlined above). It is recommended that termly subject leader time is allocated to fulfil the role
- 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 with regard to 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 Computing lead/team
- regular monitoring of the 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

Safeguarding Lead

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

They will be trained in online issues 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 safeguarding lead will refer to appendix 1.

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 PSHE 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
- collating and reviewing reports of Online Incidents (CPOMS)
- meeting regularly with Headteacher to discuss issues and subsequent actions
- taking action 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

- 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
- 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)
- when addressing any suspected misuse or Online Safety Issue, refer to appendix 1, depending on the severity

- 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 Policy
- 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:

- 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 CAIC list
- 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, work stations, 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 pupils 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 Technology Agreement which sets clear expectations for their online behaviour.
- 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 take action in response to any breach of the Online Safety Policy

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.

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 and adhere to their child's Acceptable Use Policy (Appendix 3)
- understand, acknowledge and ensure that their child adheres to school procedure relating to their use of personal devices whilst on school grounds

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

- letters, regular online safety newsletters provided by Knowsley City Learning Council, website links, publications, external agencies.
- Parents / Carer workshops, year ahead meetings and the annual learning conferences.
- 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

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).

Safeguarding, filtering and monitoring

In the event of a Safeguarding infringement or suspicion, the online incident flowchart (see appendices) 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 of 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 headteacher for evidence and reference purposes.

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 Important 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.

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 and other sources of electronic communication are monitored.
- 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

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.
- The ability to upload and share content on our main social networking site (Facebook) is reserved for a select team in school, agreed upon by the head teacher.
- Staff must take necessary precautions to protect the identity of pupils. Any images or content shared should not compromise the privacy of pupils.

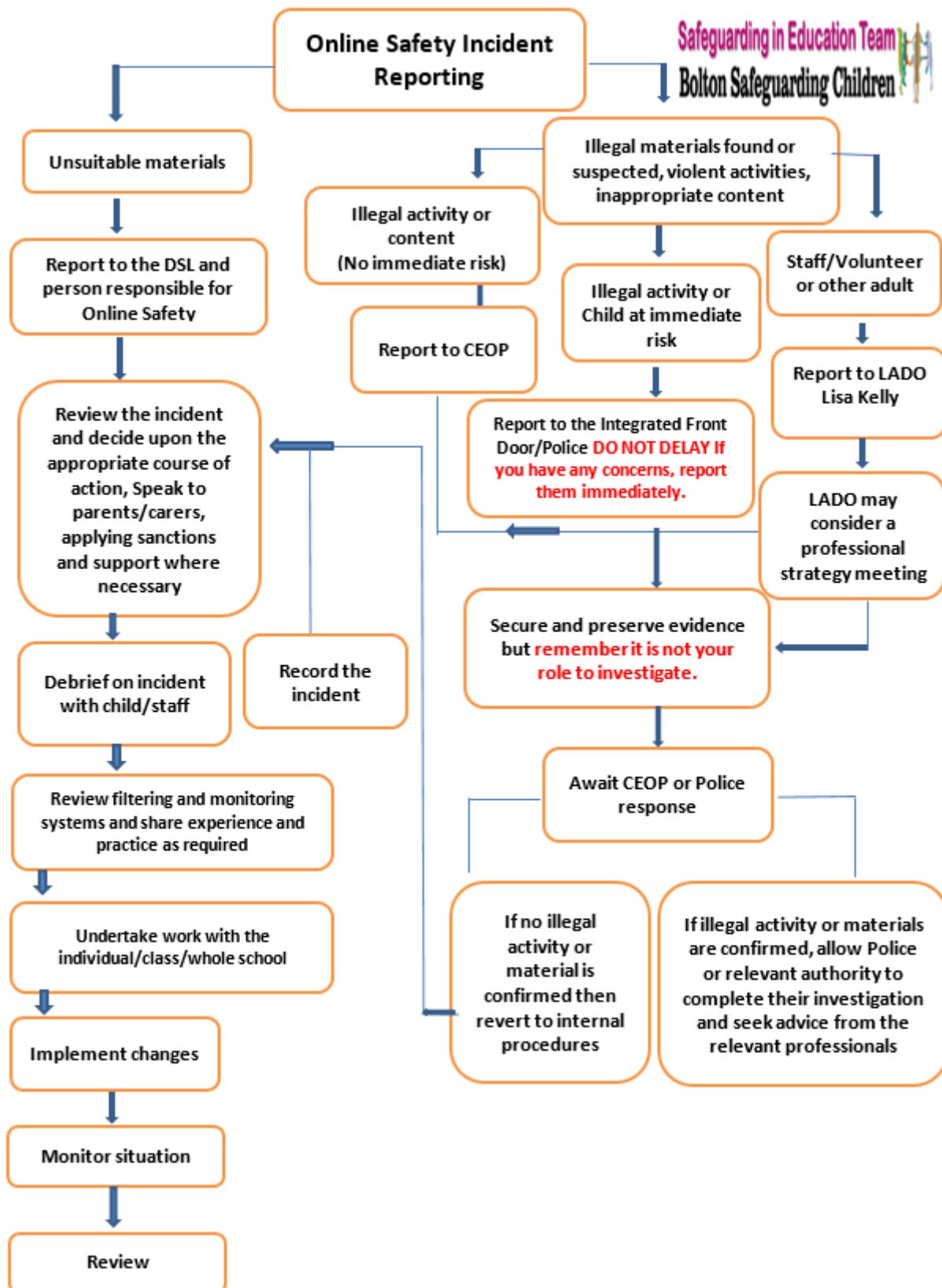
Schedule of Monitoring and Review

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 school will monitor the impact of the policy using:

- Logs of reported incidents, via CPOMS, and
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

Appendix 1



ICT Guidance for OfSTED inspection

It has been brought to our attention that during recent OfSTED inspections, questions have been asked about procedures schools are using for internet filtering and security.

We produced the notes below to assist one colleague with this and the information seemed to be helpful when answering the inspector's questions.

Therefore, I am sharing this to hopefully be of assistance should your school be inspected. Should you need any further assistance during inspection regarding ICT issues, please contact the unit and we will assist wherever possible.

For Bolton schools subscribing to Bolton Schools ICT (Bolton SICT) Broadband services, internet access is via the local authority maintained Wide Area Network. We use a central internet filtering system for all schools.

This is an industry standard solution, Sophos Universal Threat Management, the product incorporates the IWF standards.

We have this configured as per DFE guidelines, see following technical blog post:

<https://technical.bolton365.net/internet-filtering/>

The system can also be deployed at school level if required, but the standard configuration has distinct filtering levels for staff and pupils.

Filtering change requests are online and are only accepted from authorised users. Any changes are security checked before implementation.

The system provides Bolton SICT with full monitoring and reporting, these reports are available to schools when requested.

Bolton Schools ICT Broadband service also includes:

- *Email content filtering*
- *Email anti spam*
- *Secure email facilities – Multi Factor Authentication*
- *Full anti virus*
- *Encrypted document exchange*
- *2 factor remote access*
- *Industry standard firewalls to protect both WAN and school LANs*

Bolton School ICT staff that maintain these systems are all minimum Microsoft qualified and have many years industry experience.

The Inspectors have also indicated that pupils from Year 1 onwards should be using individual logins to allow monitoring of computer usage.

Some schools are already doing this, from EYFS, for network, Purple Mash and blog logon, using a four digit password.

If your school requires this facility, please contact the unit via email at contact@sict.bolton.gov.uk

For devices, such as iPads, that do not do not use network logins, we are currently looking at ways of user authentication to provide monitoring.

Sam Stoneley

Schools ICT Unit Manager

Tel: 01204 332034 Fax: 01204 332235 Email:

Sam.Stoneley@sict.bolton.gov.uk

Appendix C

Acceptable use of IT 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 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 children 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 children 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 engage in any online activity that may compromise my professional responsibilities.
- I will not support or promote extremist & terrorist 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 primarily intended for educational use and that I will only use the systems for personal use within the policies and rules set down by the school.
- 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 use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with children and parents / carers using official school systems. Any such communication will be professional in tone and manner.

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:

- 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 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 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 / academy equipment, or the equipment belonging to others.
- I will only transport, hold, disclose, or share personal information about myself or others. 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 / academy 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 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.

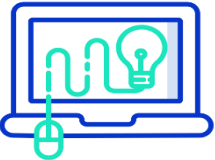
I understand that if I fail to comply with this Acceptable Use Policy, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the Police.

EYFS Technology Agreement

 My Learning Using technology @school 	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. 
 Using technology @home	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.

I understand that I need to be respectful when I use a school device.

Year 1 and Year 2 Technology Agreement

 My Learning Using technology @school 	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 I am struggling or something is not working properly. • 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.
 Using technology @home	My online world content • 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. My online world contact • 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.

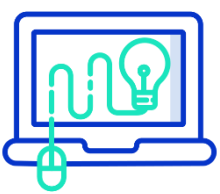
- I understand that this agreement will help me to stay safe and I agree to follow these rules.
- I also understand that I must behave respectfully and kind online to everyone when online.

Year 3 and Year 4 Technology Agreement

 My Learning	• 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. My School Accounts • 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.
 Using technology @school	My conduct as a Digital Citizen • 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.
 Using technology @home 	My online world content • 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. My online world contact • 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. My online world conduct • 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.

- I understand that this agreement will help me to stay safe and I agree to follow these rules.
- I also understand that I must behave respectfully and kind online to everyone when online.

Year 5 and Year 6 Technology Agreement

 My Learning	• 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. My School Accounts • 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.
 Using technology @school	My conduct as a Digital Citizen • 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 of anyone without their permission.
 Using technology @home 	My online world content • 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. My online world contact • 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. My online world conduct • 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. My online world commerce • 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. • 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.

- I understand that this agreement will help me to stay safe and I agree to follow these rules.
- I also understand that I must behave respectfully and kind online to everyone when online.