



# Sharples Primary School Online Safety Policy

Reviewed and Updated

Date: September 2024

## Appendices

Appendix	
1	Online Safety Incident Flowchart
2	School Technical Security Overview
3	AUP example
4	Staff Acceptable Use Policy

## Scope of the Policy

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

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

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

## 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.	To be reviewed September 2025
The implementation of this Online Safety Policy will be monitored by the:	Headteacher Governors Safeguarding Lead Computing Lead
The school will monitor the impact of the policy using:	Logs of reported incidents Monitoring logs of internet activity (including sites visited) Internal monitoring data for network activity Surveys / questionnaires of stakeholders – staff, pupils, parents
Should serious Online incidents take place, the following external persons / agencies should be informed:	Headteacher School Safeguarding Lead LADO Police <b>See Appendix 1</b>

## **Digital Resilience:**

The internet has become part of our everyday lives and is now easier to access than ever before, but using the internet can also have risks. Children and young people are more at risk of exposure to inappropriate or criminal behaviour if they are unaware of the dangers.

Digital Resilience is a term given to 'the social and emotional literacy and digital competency to positively respond to and deal with any risks they (pupils) might be exposed to when they are using social media or going online'.

Being digitally resilient is about being able to deal with any incidents that go awry online especially on social media. We aim to equip our pupils with the emotional resources needed to understand when they might be at risk online.

## **Roles and Responsibilities**

### **Headteacher:**

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

The role of the Headteacher will include:

- ensuring that all members of the school community understand and acknowledge their responsibilities in the event of a serious online allegation being made (**Appendix 1**)
- ensuring that all 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 regular subject leader time is allocated to fulfil the role
- ensuring the relevant parties receive regular monitoring reports from the Computing lead
- 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.

### **Designated Safeguarding Lead (DSL)**

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

The DSL will review and update the school's filtering and monitoring procedures, clearly defining roles and responsibilities within these processes. When assessing filtering and monitoring systems, governing bodies

and relevant parties will consider the number of children at risk and the proportionality of costs versus safety risks. The DSL will evaluate the strength and suitability of the current cyber security measures and consider improvements where necessary.

The DSL will ensure that the school's Safeguarding/ child protection policy adequately reflects its approach to online safety, including appropriate filtering and monitoring on school devices and school networks. The DSL is responsible for taking any necessary action as per the Online Safety Incident reporting flowchart (Appendix 1).

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

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

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

### **Computing Lead**

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

The role of the Computing Lead includes:

- providing advice for staff and signpost relevant training and resources
- liaising with relevant technical support teams
- reviewing reports of Online Incidents (from CPOMS)
- establishing the Online Safety Leaders and holding regular meeting with them
- communicating up-to-date Online Safety information to the wider school community

### **School Staff**

It is essential that all staff.

- receive **annual** appropriate safeguarding and child protection training, including online safety which, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- understand and acknowledge their responsibilities as outlined in this Policy.
- have read, understood and signed the Staff Acceptable Use Policy (Appendix 3)
- keep up to date with the Online Safety Policy as part of their CPD.
- will not support or promote extremist organisations, messages, or individuals.
- will not give a voice or opportunity to extremist visitors with extremist views.

- will not browse, download, or send material that is considered offensive or of an extremist nature by the school.
- have an up-to-date awareness of online matters pertinent to the children that they teach/have contact with
- report concerns and log incidents. (CPOMS)
- ensure that all digital communications with the School Community are on a professional level and only carried out using official school approved systems.
- apply this Online Safety Policy to all aspects of the Curriculum.
- share, discuss and ensure the children understand and acknowledge their responsibility to follow their age-appropriate 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.

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

### **Technical support**

The school's technical infrastructure must be secure and actively reduces the risk of misuse or malicious attack.

To facilitate this, school has purchased support from Bolton Schools ICT.

The role includes:

- Follow the [DFE digital and technology standards in schools](#)
- provide a secure Wi-Fi system – current set up with a designated school wifi for school device access and separate wifi for non-school devices and guest users
- maintaining filtering and monitoring systems
- providing filtering and monitoring alerts
- completing actions following concerns or checks to systems
- procure systems (with SLT &DSL)
- identify risk (with SLT &DSL)
- carry out reviews (with SLT &DSL)
- carry out checks (with SLT & DSL)
- ensuring that detected risks and/or misuse is reported to the DSL and nominated staff at school, via the encompass email box.
- ensuring that schools are informed of any changes to guidance or any planned maintenance.
- school technical systems will be managed and reviewed annually in ways that ensure that the school meets recommended technical requirements.
- all users will have clearly defined access rights to school technical systems and devices.
- all school network users will be assigned an individual username and password at the appropriate level of access needed for their role.
- ensuring internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the [Internet Watch Foundation](#) Child Abuse Image Content list (CAIC).
- content lists are regularly updated, and internet use is logged and regularly monitored.
- there is a clear process in place to deal with requests for filtering changes.
- provide a platform where school should report any content accessible in school but deemed inappropriate.

- ensuring appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date virus software (**Appendix 2**)

### **Pupils**

The children's learning will progress through a broad, effective and relevant Online Safety curriculum. A 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 Acceptable Use Policy (**Appendix 3**)
- be able to recognise when something makes them feel uncomfortable (butterfly feeling) and know how to report it
- accept their responsibility to respond accordingly to any content they consider as inappropriate
- understand the importance of being a responsible digital citizen and realise that the school's Online Safety Policy applies to their actions both in and out of school
- know that school will take action in response to any breach of the Online Safety Policy

### **Parents / Carers / Responsible adults**

The children's learning will progress through a broad, effective and relevant Online Safety curriculum. A pupil's learning journey will be holistic in that it will include, but is not limited to their online reputation, online bullying and their health and wellbeing.

It is essential that all pupils should:

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

### **Parents / Carers / Responsible adults**

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

Therefore, it is essential that all adults should:

- promote safe and responsible online practice and must support the school by adhering to the school's Safeguarding and Online Safety Policy in relation to digital and video images taken whilst on school premises or at school events.
- understand, acknowledge their child's Acceptable Use Policy (**Appendix 3**)
- understand, acknowledge 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, newsletters, website links, publications, external agencies
- Parents / Carer workshops

- high profile events / campaigns e.g. Safer Internet Day

### **Visitors entering school**

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

### **Useful Information**

#### **Safeguarding**

In the KCSIE 2023 there is a greater emphasis on filtering and monitoring in schools. The document stresses the importance of all staff members understanding their duties and obligations regarding online safety. Schools are advised to reflect their approach to online safety, including appropriate filtering and monitoring on school devices and networks, in their child protection policy.

‘All staff should receive appropriate safeguarding and child protection training (including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring – see para 141 for further information) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.’ [\\* DFE - KCSIE 2023](#)

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

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

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

### **Data Protection**

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

### **Communications**

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

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

### **Social Media**

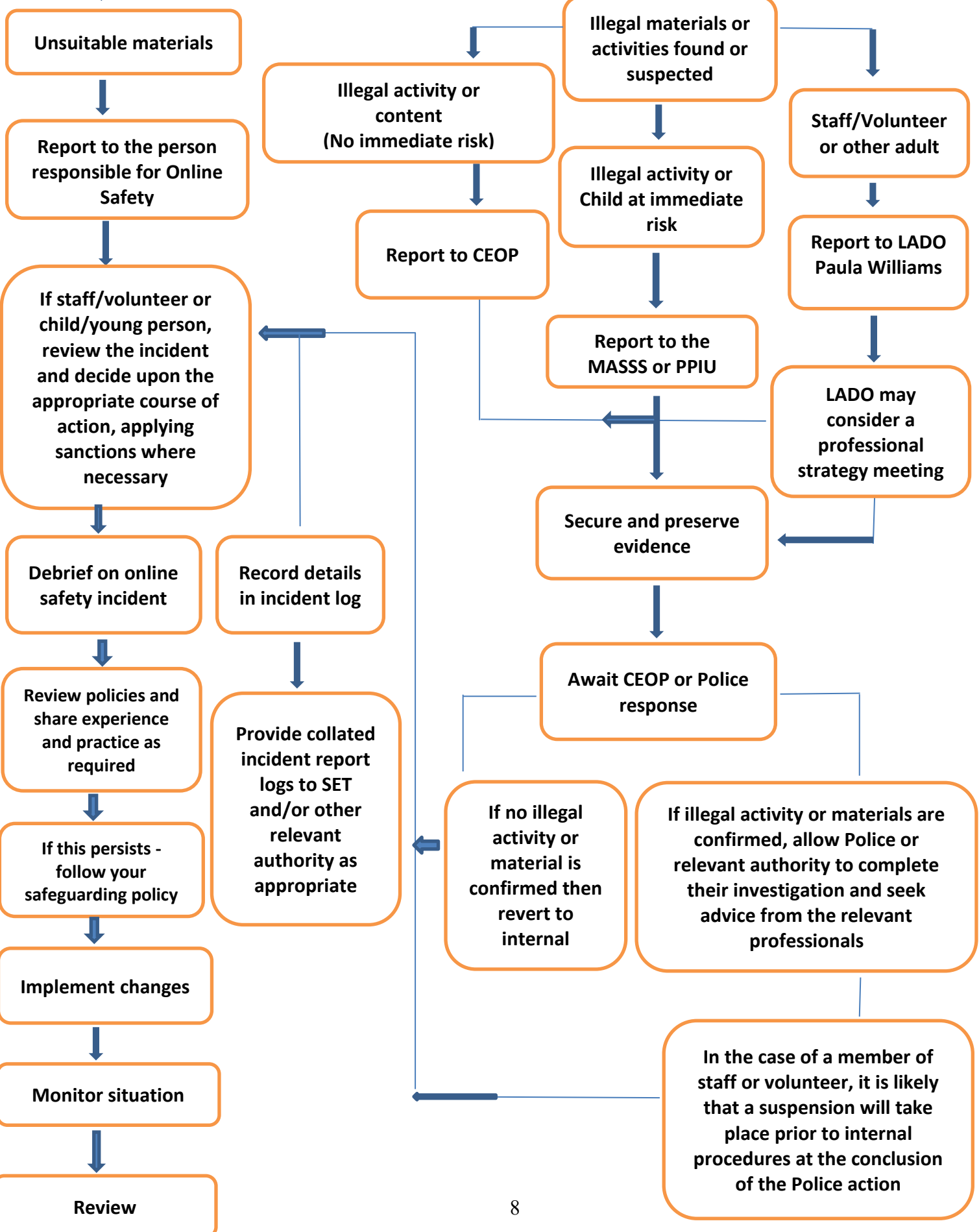
The school's use of social media is to promote the ethos of the school. It is the responsibility of all staff to ensure that the content they upload is for professional purposes only, be compliant with the school policies and protect the identity of pupils.

### **Staff Acceptable Use Policy**

Staff and Visitors are required to sign the Acceptable Use Policy. Staff understand that they must use the school IT systems in a responsible way, to ensure that there is no risk to their safety or to the safety and security of the IT systems and other users. They recognise the value of the use of technology for enhancing learning and ensure that pupils receive opportunities to gain from the use of IT. They educate the young people in their care in the safe use of technology and are a good role model in their own use of all digital technologies in their work with young people. (**Appendix 4**)



# Online Safety Incident Reporting



## **Support for Bolton Schools**

### **SET – Safeguarding in Education Team:**

- Jacqui Parkinson – Safeguarding in Education Officer – 01204 337472
- Natalie France – Safeguarding Education Social Worker – 01204 331314

**LADO:** Paula Williams - 01204 337474

**Bolton’s MASSS** – 01204 331500

**Police protection investigation unit** – 0161 856 7949

**Community Police** - 101

**EXIT Team** – 01204 337195

**Bolton Safeguarding Children’s Board:** Shona Green – 01204 337964

If there is an ICT network issues contact your school ICT provider.

If your provider is Bolton School ICT Unit – contact 01024 332034 or [contact@sict.bolton.gov.uk](mailto:contact@sict.bolton.gov.uk)

## *Appendix 2*

### **Bolton SICT Technical Security Overview**

*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.*

*Pupils from Year 1 onwards use individual logins to allow monitoring of computer usage. (for network, Purple Mash and TT Rockstars etc, using a four digit password).*

Any further information, please contact:

Sam Stoneley





Schools ICT Unit Manager

Tel: 01204 332034

Fax: 01204 332235

Email: [Sam.Stoneley@sict.bolton.gov.uk](mailto:Sam.Stoneley@sict.bolton.gov.uk)

## Year 1 and Year 2 Acceptable Use Policy

 My Learning	<ul style="list-style-type: none"> <li>• I will use school devices (PCs, laptops, tablets/ ipads) for my learning.</li> <li>• I will ask a teacher before using a device and ask for help if I can't work the device.</li> <li>• I will only use activities that a teacher has told or allowed me to use.</li> <li>• I will ask a teacher if I am not sure what to do or I think I have done something wrong.</li> <li>• I will look after the school's computing equipment and tell a teacher if something is broken or not working properly.</li> </ul>
 My Online Safety	<ul style="list-style-type: none"> <li>• I will always use what I have learned about Online Safety to keep myself safe.</li> <li>• I will tell a teacher if I see something that upsets me on the screen.</li> </ul>
 Using the Internet @school	<ul style="list-style-type: none"> <li>• I will only use the internet when the teacher says I can.</li> <li>• I will only go on websites that my teacher allows me to.</li> <li>• I will tell my teacher if I go on a website by mistake.</li> </ul>
 Using the Internet @home	<ul style="list-style-type: none"> <li>• I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details)</li> <li>• Where I have my own username and password, I will keep it safe and secret.</li> <li>• I will tell a trusted adult if I see something that upsets me on the screen.</li> </ul> <p><b>My use of Social Media and Gaming</b></p> <ul style="list-style-type: none"> <li>• I understand that certain sites and games have age restrictions to keep me safe.</li> <li>• I understand that by accessing such sites and games, I maybe putting myself at risk of accessing inappropriate content and cyberbullying.</li> </ul>

I understand that these rules help me to stay safe and I agree to follow them.  
 I also understand that if I break the rules I might not be allowed to use the school's computing equipment.

I understand that these rules, help me to stay safe and I agree to follow them.

I also understand that if I break the rules I might not be allowed to use school computing equipment.

---

**Child's Signature**

**Parents / Carers:**

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or 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.

I understand that 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 ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

**I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.**

---

**Parent/Carer's Signature**

**Date**

# **SHARPLES 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 school 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 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 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 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 should not include proper names or any other personal information about the user that might be known by others.
- I will only connect my personal devices to the school's **Guest Wi-Fi** and will ensure to 'forget' this information on all my personal devices when I cease to work, visit, be on placement or volunteer at the school.
- 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 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. (Schools / academies should amend this section to take account of their policy on access to social networking and similar sites)
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (Schools should amend this section to take account of their policy on communications with students / pupils and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Governors 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 / 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 / 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.

**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 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