Walmsley C.E. Primary School
Where getting better never stops

Bolton
Schools ICT
Putting Schools First

Walmsley C of E Primary School

Online Safety Policy

Date of Issue: November 2023
Next Review Date: November 2024

Policy Cover Note

Title of the Policy	Online Safety Policy
Summary/Reason for bringing to Governing Board for Approval	Updated to reflect current guidance
Statutory Requirement	No
Decisions to be made / recommendation on options	To be approved
Name of the author	Bolton SICT, amended by Joanna Atherton
Date written	November 2023
Date for Review	November 2024
Policy/Procedure to be published on the school website	No
Amendments/Updates	Comprehensive updates throughout

Mission Statement

As a school we pledge to:

- Be a happy school where pupils are encouraged and challenged to reach their full academic and social potential in a creative, friendly and safe Christian environment.

- Work as a partnership with pupils, their families, staff and the wider community to provide an environment of honesty, responsibility and integrity.

- Give ownership of the opportunities presented to the school family, thus enabling them to reflect on their time at Walmsley with pride.

Appendices & Policies that support this policy.

Appendix	
1	Online Safety Incident Flowchart
2	DFE Technical Standards for Bolton Schools
3	Acceptable User Agreements documents – Staff, Visitors & Volunteers
3.1-3.4	Acceptable User Agreements documents – Pupils
4	Online Incident Report Log
5	School Safeguarding Policy
6	School Data Protection Policy
7	School 'AI' guidance

Scope of the Policy

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

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

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

Development of the Policy

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

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

This Online Safety Policy was approved by the Governing Body *on:*	December 2023

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.	November 2024
The implementation of this Online Safety Policy will be monitored by the:	Headteacher Governors DSL Computing Lead
The school will monitor the impact of the policy through:	Identifying 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 Board 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**

KCSIE 2023

In the Keeping Children Safe in Education (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

Roles and Responsibilities

Headteacher:

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

The role of the Headteacher will include:

- Ensuring that all members of the school community understand and acknowledge their responsibilities in the event of a serious online allegation being made (**Appendix 1**).
- Ensuring that all staff receive suitable **annual updates** for all staff members about their responsibilities regarding online safety, filtering, and monitoring and acknowledge and understand the potential for serious child protection / safeguarding issues.
- Ensuring that the Online Safety Policy is accessible to the wider School Community (School website).
- Meet at regular intervals with the DSL to ensure the implementation of this policy (as outlined above).
- Ensuring the Governing Board receive regular monitoring reports from the DSL.
- Ensuring there are opportunities to communicate up to date Online Safety information to the wider school community.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Anti-Bullying and Behaviour Policy.

Governors:

Governors are responsible for the approval of this Online Safety Policy and for reviewing its effectiveness. This will be carried out by the Governing Board, receiving regular information about online incidents and monitoring reports.
The role of the Online Safety Governor will include:

- Regular meetings with the DSL.
- Regular monitoring of the Online Incident Log/CPOMS** (which will include anonymous details of Online Incidents Report Log **appendix 4**).
- Ensuring robust technical support is in place to keep systems safe and secure.
- Regular monitoring of filtering.
- Reporting to the Governing Board.
- Attending training for online safety where appropriate.

Designated Safeguarding Lead (DSL)

DSL takes the lead role in managing online safety, ensuring that school has clear procedures to address any safeguarding concerns and uphold the school's prevent duty obligations.
The DSL will review and update the school's filtering and monitoring procedures, clearly defining roles and responsibilities within these processes. When assessing filtering and monitoring systems, governing bodies and School Leaders 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 policy adequately reflects its approach to online safety, including appropriate filtering and monitoring on school devices and school networks.

The DSL is responsible for taking any necessary action as per the Online Safety Incident reporting flowchart (**Appendix 1**).
They will arrange regular training and provide **annual updates** for all staff members about their responsibilities regarding online safety, filtering, and monitoring and acknowledge and understand the potential for serious child protection / safeguarding issues that arise from, but not limited to:

- Sharing of personal data;
- Accessing illegal / inappropriate materials;
- Exposure to inappropriate online content;
- Inappropriate contact with adults/strangers;
- Potential or actual incidents of grooming;
- Sexting;
- Cyber-bullying.

In the event of a child protection or safeguarding incident pertaining to the above, the DSL will refer to **Appendix 1**.

<u>Computing Lead</u>
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 Project Evolve and Jigsaw frameworks are used to support the teaching of Digital Citizenship and PHSE across all year groups.
The role of the Computing Lead/team includes:

- Providing advice for staff and signpost relevant training and resources;
- Liaising with relevant outside agencies;
- Liaising with relevant technical support teams;
- As needed to support DSL reviewing reports of online incidents (**CPOMS**);
- Meeting regularly with headteacher to discuss issues and subsequent actions;
- Acting in response to issues identified;
- Communicating up-to-date online safety information to the wider school community.

<u>School Staff</u>
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 acceptable use 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 reduce the risk of misuse or malicious attack.
To facilitate this, school has purchased support from Bolton Schools ICT.
The role includes:

- Following the DFE digital and technology standards in schools;
- Providing a secure Wi-Fi system for both staff and guests within your setting;
- Maintaining filtering and monitoring systems;
- Providing filtering and monitoring reports;
- Completing actions following concerns or checks to systems;
- Procuring systems (with SLT & DSL);
- Identifying risk (with SLT & DSL);
- Carrying out reviews (with SLT & DSL);
- Carrying out checks (with SLT & DSL) 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;
- Ensuring that school technical systems will be managed and reviewed annually in ways that ensure the school meets recommended technical requirements;
- Ensuring all users will have clearly defined access rights to school technical systems and devices;
- Ensuring 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).
- Ensuring content lists are regularly updated, and internet use is logged and regularly monitored;
- Ensuring there is a clear process in place to deal with requests for filtering changes;
- Providing 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 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 3.1-4**);
- 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 and 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 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 or other criminal conduct, activity or

materials. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

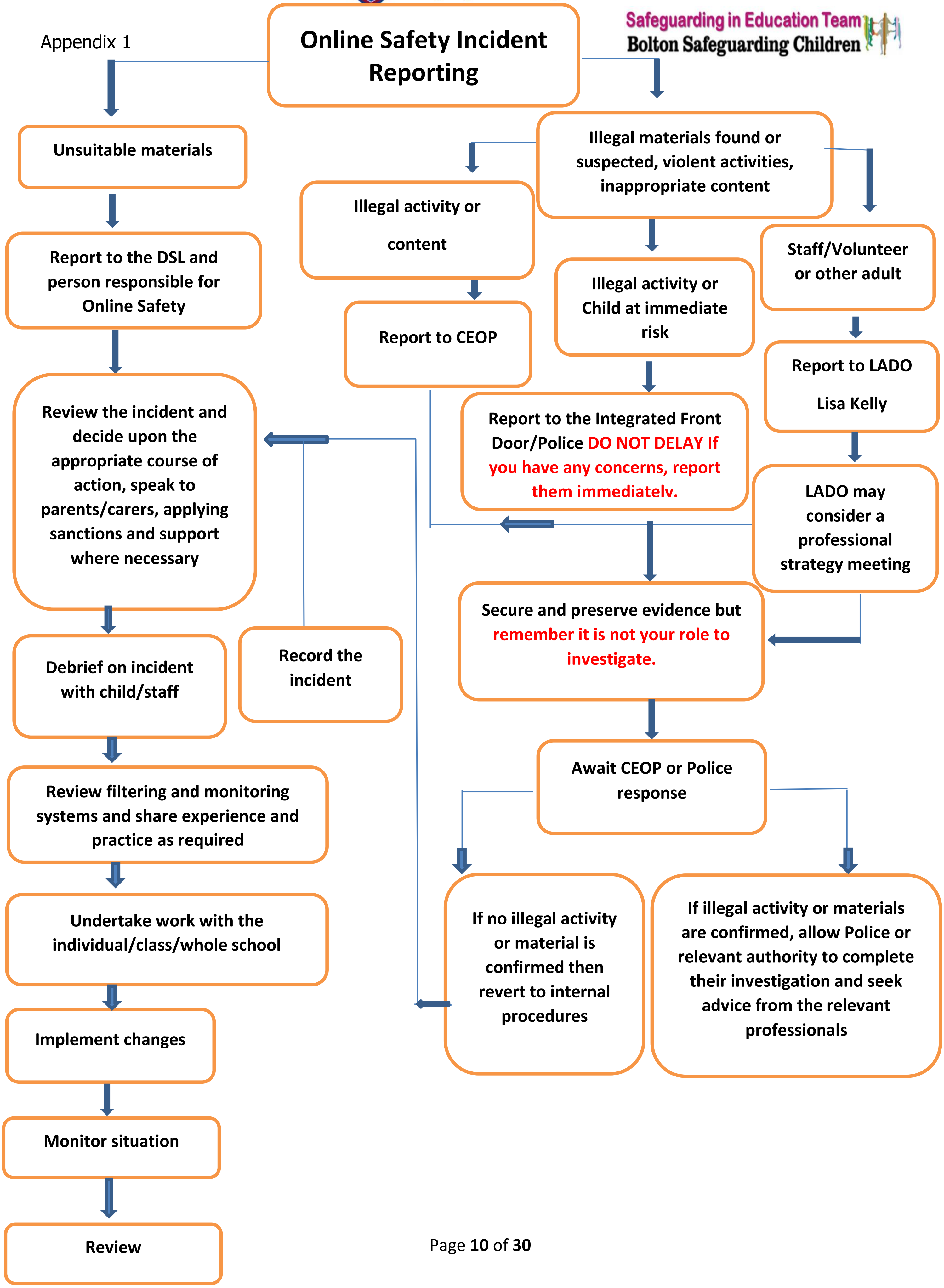
When using communication technologies the school considers the following as good practice:

- 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.

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

Record the incident

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

Illegal materials found or suspected, violent activities, inappropriate content

Illegal activity or content

Report to CEOP

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 France – 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 01204 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

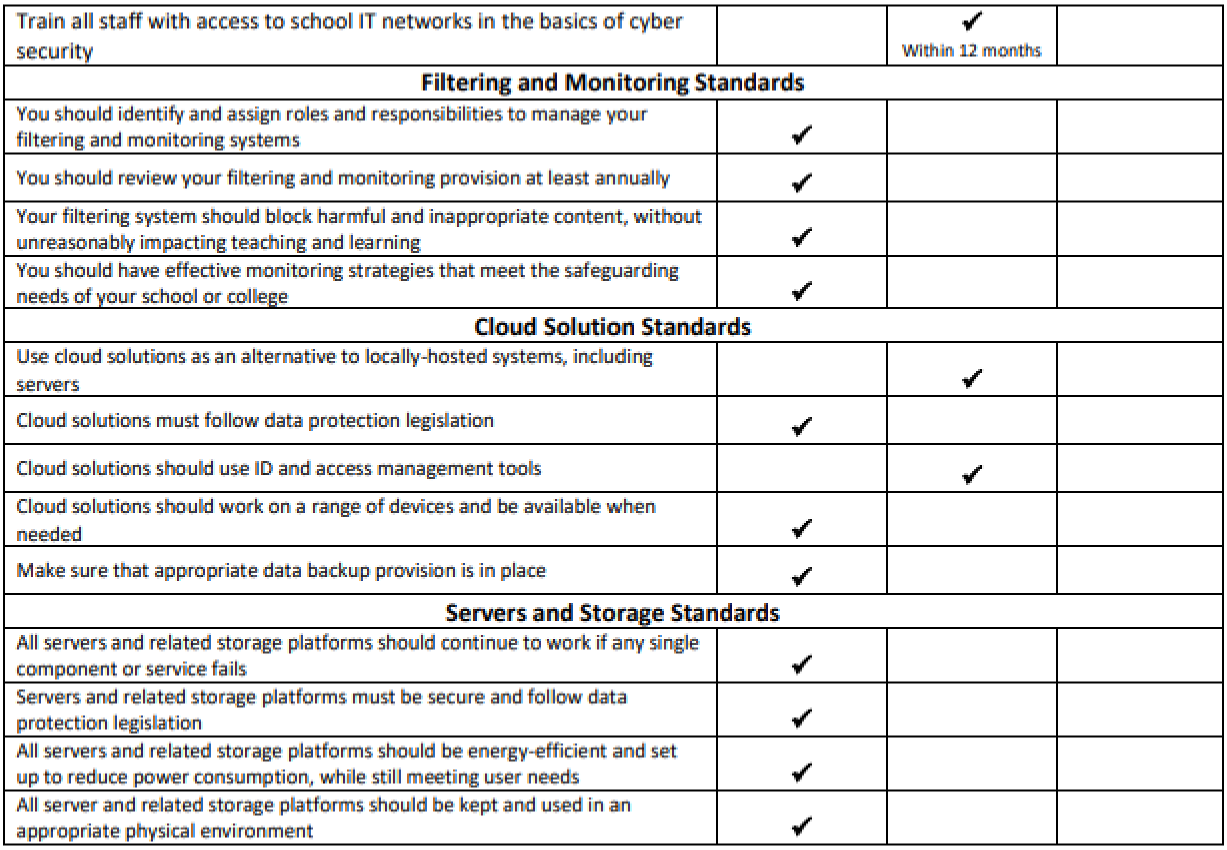
TECHNOLOGY STANDARDS FOR PRIMARY SCHOOLS 2023

CONTENTS

DFE Standards

Timetable for meeting technology standards

Technology Standard	NOW	ASAP	AT NEXT UPDATE
Broadband Internet Standards			
Schools and colleges should use a full fibre connection for their broadband service			✓
Schools and colleges should have a backup broadband connection to ensure resilience and maintain continuity of service			✓
Schools and colleges should have appropriate IT security and safeguarding systems in place, under both child and data protection legislation	✓		
Network Switching Standards			
The network switches should provide fast, reliable and secure connections to all users both wired and wireless			✓
Have a platform that can centrally manage the network switching infrastructure			✓
The network switches should have security features to protect users and data from unauthorised access			✓
Core network switches should be connected to at least one UPS to reduce the impact of outages			✓
Network Cabling Standards			
Copper cabling should be Category 6A (Cat 6A)			✓
Optical fibre cabling should be a minimum 16 core multi-mode OM4			✓
New cabling should be installed and tested in line with the manufacturer's guidance, warranty terms, and conditions			✓
Wireless Network Standards			
Use the latest wireless network standard approved by the Wi-Fi Alliance			✓
Have a fully functional signal from your wireless network throughout the school or college buildings and externally where required			✓
Have a solution that can centrally manage the wireless network			✓
Install security features to stop unauthorised access			✓
Cyber Security Standards			
Protect all devices on every network with a properly configured boundary or software firewall	✓		
Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date	✓		
Accounts should only have the access they require to perform their role and should be authenticated to access data and services		✓	
You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication		✓	
You should use anti-malware software to protect all devices in the network, including cloud-based networks		✓	
An administrator should check the security of all applications downloaded onto a network		✓	
All online devices and software must be licensed for use and should be patched with the latest security updates		✓	
You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site		✓	
Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack		✓	
Serious cyber-attacks should be reported		✓	
You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation	✓		



Train all staff with access to school IT networks in the basics of cyber security		✓ Within 12 months	
Filtering and Monitoring Standards			
You should identify and assign roles and responsibilities to manage your filtering and monitoring systems	✓		
You should review your filtering and monitoring provision at least annually	✓		
Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning	✓		
You should have effective monitoring strategies that meet the safeguarding needs of your school or college	✓		
Cloud Solution Standards			
Use cloud solutions as an alternative to locally-hosted systems, including servers		✓	
Cloud solutions must follow data protection legislation	✓		
Cloud solutions should use ID and access management tools		✓	
Cloud solutions should work on a range of devices and be available when needed	✓		
Make sure that appropriate data backup provision is in place	✓		
Servers and Storage Standards			
All servers and related storage platforms should continue to work if any single component or service fails	✓		
Servers and related storage platforms must be secure and follow data protection legislation	✓		
All servers and related storage platforms should be energy-efficient and set up to reduce power consumption, while still meeting user needs	✓		
All server and related storage platforms should be kept and used in an appropriate physical environment	✓		

This document focuses on the guidance published by DFE on meeting digital and technology standards in schools and colleagues found at: Government technology standards and guidance - GOV.UK (www.gov.uk) This summary is designed for school leaders to introduce the concept of what, at a high level, is required to take place. The document then goes on to the technical details, referencing the DFE technical standard document where they exist and providing additional detail when they do not so that a holistic solution is referenced.

Broadband Internet Standards

The Bolton Schools ICT broadband SLA provided connection exceeds the speed required in this standard. The connection is protected by a Sophos Unified Threat Management device configured at the 'edge' of the network. This is maintained and monitored by SICT. This provides Firewall and Web Filtering. From September 2023 the monitoring is provided by a product called FastVue which works alongside the web filter to provide reports and alerts.

BSICT are currently undergoing a review of this service, and whilst it is likely the product may change, this will be at least an equal match to the current solution in place, with some improvements due to advances in technology and services offered by supplies. For example, a backup connection will be provided in the next round of updates to the broadband connections in schools.

Network Switching Standards

All the switches currently available and those supplied in the last 5 years from Bolton Schools ICT meet the following requirements:

1. To provide 1Gbps connectivity to end user devices.
2. Centrally managed and monitored.

Our default switch configuration securely separates the network into 3 parts, internal secure network, external network, guest wireless network, and VOIP Telephony networks. Using VLANs prevents these separate networks from accessing each other.

Bolton Schools ICT can quote for new switches which meet the requirement for higher speeds to servers and infrastructure devices on request.

It is important to note that the ability of the switch to deliver this higher speed is dependent on the specification and quality of physical cabling, and this may also need to be upgraded to meet the separate DfE cabling standard when new networking equipment is installed.

A UPS can be provided as a power backup to your core switches as necessary, this is often of limited benefit to primary schools.

Bolton Schools ICT can survey and audit your network switches and provide recommendations to help you meet standards if not already. This can present a significant cost to school to meet, so a cost-benefit analysis would need to be carried out which we can advise on potential benefits.

Switch: Meeting digital and technology standards in schools and colleges - Network switching standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Network Cabling Standards

Having your school fully rewired with new cabling is a major expense. Most schools will have Category 5E or 6 cabling. This is suitable to provide 1Gbps connectivity to the desktop as required in the switching standards. Category 6A cabling is capable of supporting 10Gbps which is generally only used for infrastructure links.

In order to meet the network cabling standards, it is highly likely that you will need to upgrade all your network cabling. Only new build schools or those with recently installed cabling are likely to meet this standard. Bolton Schools ICT can carry out an initial basic survey to advise and assist with a cost-benefit analysis, but for a full quote or for work to be carried out you will need to engage with a cabling contractor. Bolton Schools ICT can assist you with providing the specification to the contractor and engaging in technical discussions.

Cabling: Meeting digital and technology standards in schools and colleges - Network cabling standards for schools and colleges - Guidance - GOV.UK (www.gov.uk)

Wireless Network Standards

The newest wireless access points available from Bolton Schools ICT meet the technical requirements of this standard. Bolton Schools ICT offer a wireless survey as part of quoting for the network and can arrange coverage across school as necessary. New installs will all have a segregated guest wireless network as standard, and older installs are being upgraded on a rolling basis where possible.

Schools are not required to meet this standard until your existing setup is replaced when it is either underperforming or unsupported. However, you will likely need to consider upgrading your network cabling as well at the same time, as installing a new wireless network triggers the requirement to meet the network cabling standards which present a considerable expense to school.

Cyber Security Standards

All schools utilising Bolton Schools ICT Broadband SLA are provided with an industry leading edge firewall and filtering device. They also get Sophos anti-virus as part of this SLA. This meets all the relevant requirements and is monitored and maintained as part of the SLA agreement.

Bolton Schools ICT will maintain network accounts based on requests from school and will keep a log of requests via our calls system. It is the responsibility of each school to ensure that they keep these accounts up to date and request account deactivation when staff leave. Bolton SICT can advise on how to maintain the security of your network drives so that data can only be accessed by those with permission.

Bolton Schools ICT recommend that schools use the "Cyber Security Training for School Staff" materials from the NCSC. Schools must ensure that they deliver this training every year. It is recommended that a log is kept of this training and staff completing the training download their certificate. This training should also be offered to school governors with the expectation that at least one governor completes the training every year. Any new members of staff must complete this Cyber security training as part of their induction into the school.

As part of our service into schools, Bolton Schools ICT will review the suitability, quality and effectiveness of these measures every year.

Filtering and Monitoring Standards

Schools utilising the Bolton Schools ICT broadband SLA meet this standard. Over the summer we have purchased and deployed a new monitoring system to meet the requirements for monitoring and alerts. Our existing web filter meets the filtering requirements.

Cloud Solution Standards

Schools ICT manage a Bolton-wide tenancy on Microsoft 365 for all schools utilising this service. This includes email, Teams and some schools use OneDrive/SharePoint as well. This is a hybrid solution, as schools also have a local server.

Data in our Microsoft 365 tenancy is stored within the UK or EU.

The cloud data transfer is protected behind HTTPS encryption. Logon requires multi-factor authentication when accessed outside the school secure network.

There is currently no additional backup in Microsoft 365 beyond that provided by Microsoft where deleted items can be recovered within around 30 days. Data which needs to be properly backed up must be kept on the school server.

We are investigating options for schools who wish to move more of their services into the cloud and will provide information in due course, or if you would like more information, please contact us.

Servers and Storage Standards

As part of the SLA, SICT will monitor your server for failure using Dell’s OpenManage software, and Microsoft Systems Centre Operations Manager. If a failure is detected a technician will investigate and a quote will be sent to schools for replacement hardware if not covered by warranty.

All new servers provided after September 2023 will come with multiple power supplies for redundancy, this will present an increased cost.

All servers provided by Bolton Schools ICT come with 3 year’s onsite warranty and maintenance from date of installation.

Bolton Schools ICT will keep your servers up to date and patched.

Your server should be kept in a secure location in school that is not accessible to unauthorised persons. This can either be a locked cupboard, or a secure purpose-built room. SICT can assist with moving your server if this is necessary to meet this requirement. You may need to have extra power and data points fitted, and the room or cupboard must not be used for other purposes.

Appendix 3

Staff, Visitors and Volunteers Acceptable Use Policy Template

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 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 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 uppercase characters, lowercase characters, numbers, 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 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 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 (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 system.
- 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.
- 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 Data Protection 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

Appendix 3.1

EYFS Acceptable Use 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 this agreement will help me to stay safe and I agree to follow these rules. I also understand that if I do not follow these rules, I might not be allowed to use the school's computing equipment.

Notes for School

Good Practice

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

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.

The school ICT systems has the capacity to monitor all users and that the school will contact families if they have concerns about any possible breaches of the Acceptable Use Agreement.

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

Appendix 3.2

Year 1 and Year 2 Acceptable Use 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 if I break the rules, I may not be allowed to use the school's computing equipment.

____

Child's Signature

Notes for School

Good Practice

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

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.

The school ICT systems has the capacity to monitor all users and that the school will contact families if they have concerns about any possible breaches of the Acceptable Use Agreement.

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

Appendix 3.3

Year 3 and Year 4 Acceptable Use 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 if I break the rules or behave inappropriately online in school, I may not be allowed to use the school's computing equipment.

____

Child's Signature

Notes for School

Good Practice

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

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.

The school ICT systems has the capacity to monitor all users and that the school will contact families if they have concerns about any possible breaches of the Acceptable Use Agreement.

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

Appendix 3.4

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 if I break the rules or behave inappropriately online in school, I may not be allowed to use the school's computing equipment.

____

Child's Signature

Notes for School

Good Practice

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

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.

The school ICT systems has the capacity to monitor all users and that the school will contact families if they have concerns about any possible breaches of the Acceptable Use Agreement.

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

Appendix 4

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

Appendix 5

School safeguarding policy

Appendix 6

School Data Protection Policy

Appendix 7

AI Usage Guidelines