



Oxford Grove Primary School  
Online Safety Policy



September 2023

To be reviewed  
September 2024

## **Appendices & Policies that support this policy.**

<b>Appendix</b>	
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 Data Protection Policy
6	Artificial Intelligence Usage Guidelines 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).

## **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.

- *Computing Subject Lead*
- *Designated Safeguarding Lead*
- *Senior Leadership Team*
- *Safeguarding Governor*

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

September 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.

September 2024

The implementation of this Online Safety Policy will be monitored by the:

Head teacher  
DSL has responsibility for online safety, in liaison with all others listed in the section  
Senior Leadership Team  
Safeguarding Governor  
School Business Manager with accountability for technology  
Computing Lead

The school will monitor the impact of the policy using:

Identify children at greater risk of harm.  
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  
Online Safety Risk Assessment using 360 template-successfully completed, resulting in the 360 Online Safety Mark.

Governing Body will receive a report on the implementation of the Online Safety Policy generated by the monitoring group at regular intervals:	Termly where appropriate
Should serious Online incidents take place, the following external persons / agencies should be informed:	Head teacher School Designated Safeguarding Lead LADO Police <b>See Appendix 1</b>

## **KCSIE 2023**

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](#)

## **Roles and Responsibilities**

### **Head teacher:**

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

The role of the Head teacher will include:

- ensuring that all members of the school community understand and acknowledge their responsibilities in the event of a serious online allegation being made (**Appendix 1**)
- ensuring that all 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 Safeguarding Governor receives regular monitoring reports from the DSL in liaison with the Computing lead and the Business Manager.
- ensuring there are opportunities to communicate up to date Online Safety information to the wider school community.

The Education and Inspections Act 2006 empowers Head teachers 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 Positive 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 Safeguarding Governor, receiving regular information about online incidents and monitoring reports.

The role of the Safeguarding Governor will include:

- regular meetings with the DSL/ Computing lead
- regular monitoring of the E-Safety Incident Logs/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 on the advice of Bolton School's ICT, clearly defining roles and responsibilities within these processes. When assessing filtering and monitoring systems, the Head teacher, DSL and Safeguarding Governor will consider the number of children at risk and the proportionality of costs versus safety risks. The DSL, in liaison with the School's Business Manager and Schools ICT, will evaluate the strength and suitability of the current cyber security measures and consider improvements where necessary.

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

### **Computing Lead / Team**

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

The role of the Computing Lead includes:

- providing advice for staff and signpost relevant training and resources
- liaising with relevant outside agencies
- liaising with relevant technical support teams
- supporting the DSL reviewing reports of Online Incidents (**Appendix 4 / CPOMS**)
- meeting regularly with Head teacher and the DSL to discuss issues and subsequent actions.
- acting in response to issues identified
- communicating up-to-date Online Safety information to the wider school community

### **School Staff**

It is essential that all staff:

- receive **annual** appropriate safeguarding and child protection training, including online safety which, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- understand and acknowledge their responsibilities as outlined in this Policy.
- have read, understood and signed the Staff Acceptable Use Policy (**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. (**Appendix 4** / 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 reduces the risk of misuse or malicious attack. To facilitate this, school has purchased support from Bolton Schools ICT.

The role of Technical Support Staff includes:

- Follow the [DFE digital and technology standards in schools](#)
- provide a secure Wi-Fi system for both staff and guests with in your setting
- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- 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 Head teacher at school.
- ensuring that schools are informed of any changes to guidance or any planned maintenance.
- school technical systems will be managed and reviewed annually in ways that ensure that the school meets recommended technical requirements.
- all users will have clearly defined access rights to school technical systems and devices.
- all school network users will be assigned an individual username and password at the appropriate level of access needed for their role.
- ensuring internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the [Internet Watch Foundation](#) 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 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 Online Safety Promise. (**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, 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 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 Head teacher 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's Data Protection Policy (**Appendix 5**) and the Information Management Policy.

## Communications

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

- The Office 365 school email service is safe and secure and is monitored. Users should be aware that email communications 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 school 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.

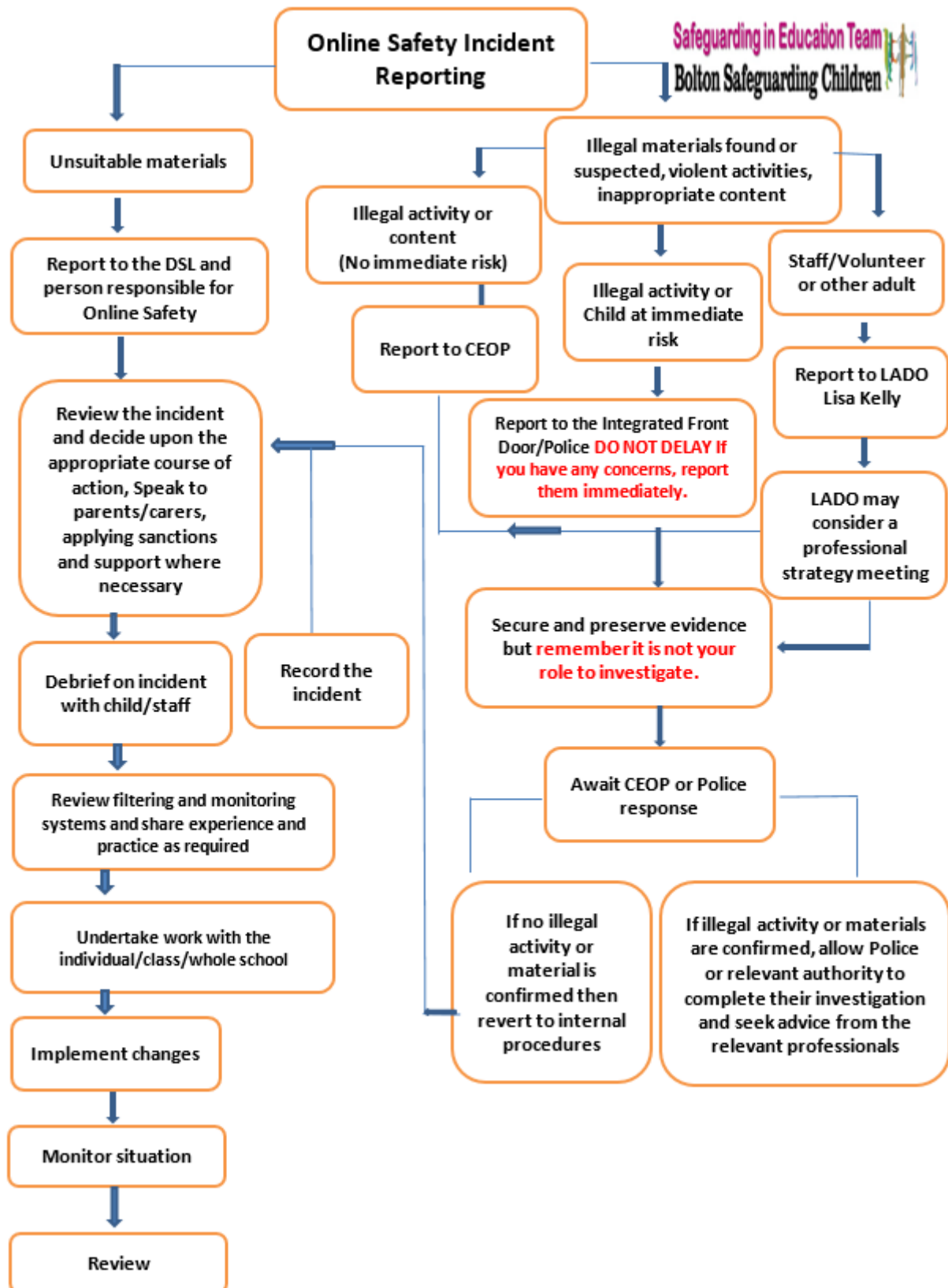
## Social Media

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, including the school's Social Media Policy, and protect the identity of pupils.

 <b>NCA</b> Young people can report concerns about child sexual abuse and exploitation to NCA	 <b>Report Remove</b> A free tool that allows children to report nude or sexual images and videos of themselves that they think might have been shared online	 <b>ChildLine</b> A free, private and confidential service where CYP can talk about anything to a trained counsellor, online or on the phone	 <b>NSPCC Report Abuse in Education</b> The Report Abuse in Education helpline offers support and guidance to CYP and who have experienced or witnesses sexual harassment or abuse in schools
--	--	--	--



## Appendix 1



# 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 01024 332034 or [contact@sict.bolton.gov.uk](mailto: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 SEPTEMBER 2023

## **Contents**

Timetable for meeting Technology standards  
Executive summary

**DFE Standards**  
Broadband Internet Standards  
Network Switching Standards  
Network Cabling Standards  
Wireless Network Standards  
Cyber Security Standards  
Filtering and Monitoring Standards  
Cloud Solution Standards  
Servers and Storage Standards

## Timetable for meeting Technology Standards

<b>Technology Standard</b>	<b>NOW</b>	<b>ASAP</b>	<b>AT NEXT UPDATE</b>
<b>Broadband Internet Standards</b>			
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	✓		
<b>Network Switching Standards</b>			
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			✓
<b>Network Cabling Standards</b>			
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			✓
<b>Wireless Network Standards</b>			
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			✓
<b>Cyber Security Standards</b>			
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	
<b>Filtering and Monitoring Standards</b>			
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	✓		
<b>Cloud Solution Standards</b>			
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	✓		
<b>Servers and Storage Standards</b>			
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	✓		

## Executive Summary

This document focuses on the guidance published by DFE on meeting digital and technology standards in school and colleagues found at: [Government technology standards and guidance - GOV.UK \(www.gov.uk\)](https://www.gov.uk/government/standards/government-technology-standards-and-guidance)

This summary is designed for school leaders to introduce the concept of what, at a high level, may be required. You should read the standards alongside this document. As every school is unique, this document is to be treated as a general overview. If you have specific questions, please log a call via the

usual method. As part of our service, each school covered by our SLA will be visited this year with a view to providing a full audit based on these standards. We will provide you with customised guidance for your school on the most appropriate and cost-effective improvements, within your budgetary restrictions. This document will be updated over time to reflect the ongoing work being carried out by Bolton Schools ICT.

## Broadband Internet Standards

Schools and colleges should use a full fibre connection for their broadband service.

The Bolton Schools ICT Broadband SLA connection meets or exceeds the speed requirements of this standard. Secondary schools have a full fibre connection, however for primary schools this would not be cost-effective. As the required speeds for primary schools are exceeded, we feel this is the most cost-effective solution to meet the spirit of the standards.

Schools and colleges should have a backup broadband connection to ensure resilience and maintain continuity of service.

Bolton Schools ICT 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 suppliers. As part of this, a backup connection will be provided in the next round of updates to the broadband connections in schools.

Schools and colleges should have appropriate IT security and safeguarding systems in place, under both child and data protection legislation.

The Bolton Schools ICT Broadband SLA connection is protected by a Sophos Unified Threat Management device configured at the 'edge' of the network. This is maintained and monitored by Bolton Schools ICT. 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.

## Network Switching Standards

The network switches should provide fast, reliable and secure connections to all users both wired and wireless.

All the switches currently available and those supplied in the last 5 years from Bolton Schools ICT can provide 1Gbps connection to the desktop. All PoE (Power over Ethernet) switches supplied in the last 5 years meet the requirements.

Not every switch provided can link at the high speeds in the standards, as these can be very expensive and, in most cases, this kind of speed is not necessary in a primary school. Bolton Schools ICT will advise you if investing in these switches would be of benefit to your school during the audit. 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.

Have a platform that can centrally manage the network switching infrastructure.

Bolton Schools ICT monitor the main switch in each school via SolarWinds which provides alerts of downtime on this switch. Existing switches are added to central management where possible. All new switches provided by Bolton Schools ICT are capable of being centrally managed via cloud-based admin tools and will be managed by Bolton Schools ICT as part of our service.

The network switches should have security features to protect users and data from unauthorised access. 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.

Core network switches should be connected to at least one UPS to reduce the impact of outages.

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

## 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.

Having your school fully rewired with new cabling is a major expense. Most schools will have copper 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. The same applies to fibre-optic cabling as to copper cabling, having this replaced can be expensive.

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 if you are having new cabling installed.

## Wireless Network Standards

Use the latest wireless network standard approved by the Wi-Fi Alliance.

The newest wireless access points available from Bolton Schools ICT meet the technical requirements of this standard.

Have a fully functional signal from your wireless network throughout the school or college buildings and externally where required.

Bolton Schools ICT offer a wireless survey and can arrange coverage across school as necessary.

Have a solution that can centrally manage the wireless network.

All wireless networking installed in the last 5 years from Bolton Schools ICT meets this standard.

Install security features to stop unauthorised access.

New installs will all have a segregated guest wireless network as standard, and older installs are being upgraded on a rolling basis where possible. The secure school network is being upgraded with a more complex password as well. As technology allows, we will upgrade the network security to the latest WPA3 standards.

## Cyber Security Standards

Protect all devices on every network with a properly configured boundary or software firewall.

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.

Network devices should be known and recorded with their security features enabled, correctly configured and kept up to date.

Bolton Schools ICT will keep records of network devices purchased from us and will ensure that they are configured to meet this standard.

Accounts should only have the access they require to perform their role and should be authenticated to access data and services.

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 Schools ICT can advise on the security of your network drives so that data can only be accessed by those with permission. This is especially important for SLT drives and SENCO materials.

You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication.

All staff accounts have multi-factor authentication enabled for logging on outside the school secure network via Remote Access or Office 365.

You should use anti-malware software to protect all devices in the network, including cloud-based networks.

All school computers and laptops purchased or configured by Bolton Schools ICT are protected by Sophos Anti-Virus as part of the SLA. This does not apply to third-party or personal devices which need to be configured before being considered secure enough to connect to the school secure network. These devices can however be connected to the guest wireless network which is securely separated from the school secure network.

An administrator should check the security of all applications downloaded onto a network.

Bolton Schools ICT recommend that you should ask your on-site technician in the first instance to ensure that any applications you wish to use meet this standard.

All online devices and software must be licensed for use and should be patched with the latest security updates.

Bolton Schools ICT recommend that you should ask your on-site technician in the first instance to ensure that any software or devices you wish to use meet this standard before you connect them to your network or download them. You should no longer be using outdated operating systems such as Windows 7 or Windows XP.

You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site.

Schools which subscribe to the backup section of the SLA will meet this requirement. Our backup solution maintains an off-site backup.

Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber-attack.

As part of the RPA Cyber Cover insurance, you should have this in place. Bolton Schools ICT can provide guidance materials on this if required.

Serious cyber-attacks should be reported.

If Bolton Schools ICT detect a cyber-attack, we will alert schools and we can advise and assist with the next steps to take to meet this standard as you will need to report it.

You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation.

This should already be in place. We can provide advice and assistance with this if you need more information.

Train all staff with access to school IT networks in the basics of cyber security

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

You should identify and assign roles and responsibilities to manage your filtering and monitoring systems.

In the new release of KCSIE, there are some vastly increased requirements for schools in terms of monitoring and alerting for the web filtering systems already in place. To meet these new guidelines, we have implemented a new alerting system, which runs alongside the Sophos Web Filtering service currently being used in schools.



In general terms, there is a greater responsibility on the DSL within school to monitor and investigate (if necessary) any potential safeguarding issues regarding the internet provision.

As part of our service, Bolton Schools ICT will provide you with a pack of information which will assist you in assigning these roles and responsibilities. Over time this pack will be added to and improved and will include pre-filled responses and simpler language.

You should review your filtering and monitoring provision at least annually.

Bolton Schools ICT will review the provision we provide on a regular basis to ensure it meets or exceeds relevant standards and legal requirements. As part of the audit visit, we will provide you with a report on which categories are blocked/allowed on your web filter, and how the monitoring system is configured.

There is an update below on the improvements we have made.

Over summer, Bolton Schools ICT have implemented a new monitoring system called FastVue to assist schools in meeting these requirements. The new monitoring system will send emails to the school designated DSL staff, notifying of any 'Unacceptable' internet browsing, as well as any unsuitable keyword searches that may take place. The school DSL will then need to determine any further action that may be required.

By default, the notification emails will be sent to the 'Encompass' mailbox within school. We can also send the notification emails to other staff members if required, however the Encompass email will be the 'default' as standard.

From September, we will work with your onsite technician (where available) to identify the exact steps and requirements necessary for each school, however if you have any specific queries or requirements not detailed above, then please log a call in the usual manner and we will assist however we can.

For notifications to be configured correctly, please complete the form by clicking on [this link](#). We will not be able to send notifications without this information.

The new alerting system will only report usernames where the device is logged on as a school user account, e.g. 123smithj. Any non-authenticating devices such as iPads will only show a device/machine name or IP address.

There are a few technical steps which need to be implemented to make this work fully, and it is worth noting that we cannot implement this on any third-party devices (you can manually configure this on each device if you wish – however as this will predominantly be staff personal devices, this would be for you to decide.)

Bolton Schools ICT will configure this for school owned laptops and computers which are connected to the schools Active Directory – which means you are able to logon with your school username and password. We will also configure this for iPads which are managed through our provided JAMF mobile device management.

Devices which will not work or will need to be configured by school or your on-site technician include:

- Staff phones – *should only be connecting to guest Wi-Fi.*
- Non-AD authenticating machines (e.g., staff personal laptops) – *should only be connecting to guest Wi-Fi.*
- Non Schools ICT managed iPads - *can be moved to guest Wi-Fi or school can install certificate manually.*
- Android Tablets - *should be moved to guest Wi-Fi .*
- LBQ tablets - *should be removed completely due to age/security considerations.*
- Alexa/Google smart assistants - *should be moved to guest Wi-Fi.*
- Any third-party devices that use https call back (e.g., printers/inventory/door control etc....) - *can be moved to guest Wi-Fi/external.*

The keyword search monitoring will only be enabled for school owned devices which are connected to the internal network. Any devices connected to the 'Guest' Wi-Fi will not be included in this, however as this is likely to be staff/visitor personal devices then this should not be an issue.

The keyword searches rely on a certificate being installed on the device to enable full scanning. Any device connected to the internal network without this certificate will not be subject to the keyword scanning and will likely show errors on general web browsing.



The central configuration is in place, however there are a few steps needed to fully implement this, namely the certificate issue and configuration against the new wireless network configurations which have also taken place.

Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning.

Bolton Schools ICT Broadband SLA schools have web filtering provided by Sophos. They are a member of the Internet Watch Foundation; they are signed up to the Counter Terrorism Internet Referral Unit list and they block access to illegal content including CSAM.

The Sophos UTM is based on the edge of the network, meaning ALL traffic out to the internet must pass through the UTM therefore it protects all devices in school. This includes mobile and app content.

SafeSearch is enforced in all schools on all devices and is not capable of being turned off by the end-user.

The blocked categories are configured for appropriate filtering for each level of user (staff/pupil) and devices which cannot be logged into are always given the pupil level filtering.

Your guest wireless network can be configured to provide three levels of filtering: Staff with social media, Staff or Pupil. This is applicable to anyone using the guest network. You will be contacted to ask which level of filtering you require, but by default we have selected Pupil on schools with a guest wireless.

You should have effective monitoring strategies that meet the safeguarding needs of your school or college.

The new FastVue monitoring system will work alongside physical monitoring and classroom management by providing alerting on unacceptable browsing and unsuitable keyword searches. Bolton Schools ICT are constantly working to improve offerings to assist with this, and we will provide information on new monitoring solutions as they are rolled out.

FastVue will email alerts and fortnightly reports to the designated email address, or the Encompass email address by default. These reports are intended to be easily understood by the DSL and non-technical staff. Bolton Schools ICT can assist with understanding these reports.

## Cloud Solution Standards

Use cloud solutions as an alternative to locally hosted systems, including servers.

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. 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.

Cloud solutions must follow data protection legislation.

Data in our Microsoft 365 tenancy is stored within the UK or EU. The cloud data transfer is protected behind HTTPS encryption.

Cloud solutions should use ID and access management tools.

Logon requires multi-factor authentication when accessed outside the school secure network.

Cloud solutions should work on a range of devices and be available when needed.

Microsoft 365 works in web browsers which are available on many devices such as laptops, tablets, mobile phones and personal computers.

Make sure that appropriate data backup provision is in place.

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.

## Servers and Storage Standards

All servers and related storage platforms should continue to work if any single component or service fails.

All servers provided by Bolton Schools ICT have RAID configured, which means if one of the disks in the server fails, the others will continue to work, and when this disk is replaced, it will be brought back into full operation with no data loss.

As part of the SLA, Bolton Schools ICT 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 servers provided by Bolton Schools ICT come with 3 year's onsite warranty and maintenance from date of installation.

All schools subscribed to the backup section of the SLA meet the requirements to back up data.

All new servers provided after September 2023 will come with a 5-year warranty and multiple power supplies for redundancy, this will present an increased cost up-front but will mean you can extend the time between server upgrades to lower total cost.

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

All servers and related storage platforms should be energy-efficient and set up to reduce power consumption, while still meeting user needs.

Your server meets the energy star requirements. Over the coming year we will review the configuration of servers to see if any energy saving can be made without impacting service to schools.

Servers and related storage platforms must be secure and follow data protection legislation.

As part of the audit visit, Bolton Schools ICT will work with your DPO to ensure that your network drive security is configured to your requirements. You are responsible for ensuring that you meet the data protection legislation on the areas including data retention and sharing.

All server and related storage platforms should be kept and used in an appropriate physical environment.

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 with adequate cooling. Bolton Schools ICT 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. As part of the audit visit, we will assist you with selecting the most appropriate and cost-effective option.

### **Appendix 3**

#### **Oxford Grove Primary School Staff, Governor and Volunteer Acceptable Use Agreement**

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 Agreement is intended to ensure:**

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

The school will try to ensure that staff, governors 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, governors and volunteers to agree to be responsible users.

#### **Acceptable Use Agreement Declaration**

I understand that I must use 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 IT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of IT. I will, where possible, 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 children.

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, blogs.) 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 not** use the systems for personal or recreational use in line with the policies and rules set down by the school.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of to the Senior Leadership Team
- 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 express permission.
- I will communicate 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 GDPR compliant Information Management Policy on the use of digital / video images and parental declarations on the use of digital / video images.
- Where these images are published (e.g. on the school website / blog), it will not be possible to identify by name, or other personal information, the children who are featured.
- I will not use my personal equipment to record images in school.
- I will restrict the use of mobile phones/smart devices(including watches) for personal telephone calls or texts to break time or lunchtime periods in the staff room or when children are off the school premises
- I will not use school devices to access chat and social networking sites in school in accordance with the school's Social Media policy.
- 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.

#### **Staff passwords:**

- **All staff users will be provided with a username and password** by Bolton Schools IT who will keep an up to date record of users and their usernames.
- The password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters must not include proper names or any other personal information about the user that might be known by others.
- I will not disclose my username or password to anyone else, nor will I 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 see it. I will inform Senior Leadership immediately, if I believe the security of my password has been compromised.

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. To support this:

- I will not 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 use my personal mobile devices (PDAs / laptops / mobile phones/smart watches) in school for any school business.
- 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 use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to illegal or inappropriate materials.
- I will not (unless I have permission) make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- 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 permission has been granted by the Computing lead.
- 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 and Freedom of Information Policy and Information Management Policy. Where digital personal data is transferred outside the secure local network, it must be encrypted or sent by the secure email system. 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 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 Agreement** 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 Agreement, I could be subject to disciplinary action.**  
This could include a warning, a suspension, referral to the Governing Board or the Local Authority, and in the event of illegal activities the involvement of the police.


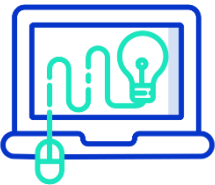


I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Governor/Volunteer Name

Signed

Date

## EYFS Online Safety Promise

 <p><b>My Learning</b></p> <p><b>Using technology @school</b></p> 	<ul style="list-style-type: none"> <li>• My conduct as a Digital Citizen</li> <li>• 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.</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 me to use.</li> <li>• I will ask a teacher if I am not sure what to do or think I have done something wrong.</li> <li>• I can talk about my digital footprint and will try to use what I have learned about Online Safety in school.</li> <li>• I know that there are rules that I need to follow to help me keep safe and healthy online at <b>school</b> when using technology.</li> <li>• I will only use the internet when the teacher says I can.</li> <li>• I will tell my teacher if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.</li> </ul> 
 <p><b>Using technology @home</b></p>	<p><b>My online world content</b></p> <ul style="list-style-type: none"> <li>• I know that there are rules that I need to follow to help me keep safe and healthy online at <b>home</b> when using technology.</li> <li>• I will tell a trusted adult if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.</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.

\_\_\_\_\_  
 Child's Name

\_\_\_\_\_  
 Class

\_\_\_\_\_  
 Date

## **Parents / Carers:**

Please encourage your child 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 Online Safety Promise.

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

**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.**


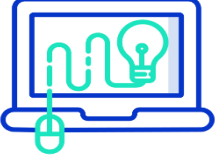

---

**Parent/Carer's Signature**

---

**Date**

## Year 1 and Year 2 Online Safety Promise

 <p><b>My Learning</b></p> <p><b>Using technology @school</b></p> 	<p>My conduct as a Digital Citizen</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• I know I need to follow our online safety rules to help me keep safe and healthy online at school when using technology.</li> <li>• I will only use activities that my teacher has told or allowed me to use.</li> <li>• I will be kind online, so I do not upset my friends.</li> <li>• I can talk about my digital footprint and will use what I have learned about Online Safety in school to search safety.</li> <li>• I will tell my teacher if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.</li> </ul>
 <p><b>Using technology @home</b></p>	<p>My online world content</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 may be putting myself at risk of cyberbullying.</li> <li>• I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.</li> </ul> <p>My online world contact</p> <ul style="list-style-type: none"> <li>• Where I have my own username and password, I will keep it safe and secret.</li> <li>• I will not share personal information about myself when on-line (names, addresses, telephone numbers, age, gender, school details)</li> <li>• I will tell a trusted adult if I see something or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.</li> </ul>

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 Name

\_\_\_\_\_  
Class

\_\_\_\_\_  
Date

## **Parents / Carers:**

Please encourage your child 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 Online Safety Promise.

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

**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**



# Year 3 and Year 4 Online Safety Promise

 <p><b>My Learning</b></p>	<ul style="list-style-type: none"> <li>• 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.</li> </ul> <p><b>My School Accounts</b></p> <ul style="list-style-type: none"> <li>• I will keep my usernames and passwords safe and secure - I will not share them.</li> <li>• I will not use anyone else's username and password.</li> <li>• I will only use apps, programs, or websites that my teacher has told me to use.</li> <li>• I will save only schoolwork on the school network.</li> </ul>
 <p><b>Using technology @school</b></p>	<p><b>My conduct as a Digital Citizen</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• I will respect other people's work and property and will not access, copy, delete any other user's files.</li> <li>• I know that I should check the content on websites as not everything is real or true.</li> </ul>
 <p><b>Using technology @home</b></p> 	<p><b>My online world content</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 may be putting myself at risk of accessing inappropriate content and cyberbullying.</li> <li>• I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.</li> </ul> <p><b>My online world contact</b></p> <ul style="list-style-type: none"> <li>• I will be aware that new friends made online may not be who they say there.</li> <li>• I will be aware of what information cannot be shared between my friends.</li> <li>• I will be polite and responsible when I communicate with others online.</li> <li>• I will not use inappropriate language and I understand that others may have different opinions than me.</li> </ul> <p><b>My online world conduct</b></p> <ul style="list-style-type: none"> <li>• I understand that spending too much time online is not always good for me.</li> <li>• I understand that content I share online can still be there even after I have deleted it.</li> <li>• I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.</li> <li>• 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.</li> </ul>

- 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 name \_\_\_\_\_

Child's signature \_\_\_\_\_

## **Parents / Carers:**

Please encourage your child 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 Online Safety Promise.

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

**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**

## Year 5 and Year 6 Online Safety Promise

 <p><b>My Learning</b></p>	<ul style="list-style-type: none"> <li>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.</li> </ul> <p><b>My School Accounts</b></p> <ul style="list-style-type: none"> <li>I will keep my usernames and passwords safe and secure - I will not share them.</li> <li>I will not use anyone else's username and password.</li> <li>I will only use apps, programs, or websites that my teacher has told me to use.</li> <li>I will log off or shut down a computer when I have finished using it.</li> </ul>
 <p><b>Using technology @school</b></p>	<p><b>My conduct as a Digital Citizen</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> <li>I will not take or distribute images of anyone without their permission.</li> </ul>
 <p><b>Using technology @home</b></p> 	<p><b>My online world content</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 may be putting myself at risk of accessing inappropriate content and cyberbullying.</li> <li>I will tell a trusted adult if I see content or somebody has made me feel sad, uncomfortable, embarrassed, or upset on the screen.</li> </ul> <p><b>My online world contact</b></p> <ul style="list-style-type: none"> <li>I will be aware that new friends made online may not be who they say there.</li> <li>I will be aware of what information cannot be shared between my friends.</li> <li>I will be aware of regularly checking privacy on apps to keep me safe.</li> <li>I will not arrange to meet people off-line that I have communicated with on-line, unless it is under the supervision of my parent/carer.</li> </ul> <p><b>My online world conduct</b></p> <ul style="list-style-type: none"> <li>I understand that spending too much time online is not always good for me.</li> <li>I will be polite and responsible when I communicate with others online.</li> <li>I will not use inappropriate language and I understand that others may have different opinions than me.</li> <li>I understand that content I share online can still be there even after I have deleted it.</li> </ul> <p><b>My online world commerce</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>

- 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 name \_\_\_\_\_

Child's signature \_\_\_\_\_

## **Parents / Carers:**

Please encourage your child 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 Online Safety Promise.

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

**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**

## Appendix 4

# Online Safety Log Incident Form

Name of adult/s writing log		Day, date, time of incident		Device and number		Pupil Involved and Class	
		Day- Date- Time-					
Adult(s) supervising at the time of the incident		Area of school where incident took place		Name(s) of children affected by the incident			
Details of incident.							
Actions Taken - warnings/reminders/reference made to individual behaviour targets/guidance given to pupil/time out/choices discussed							
Details of Senior Leadership involvement							
Parental involvement		Line Manager Involvement		Head teacher involvement			
Yes	No	Yes	No	Yes	No		
Formal Actions Taken							
Break-time deprivation		Lunchtime deprivation		Fixed term exclusion			
Yes (5 min)	No	Yes (How long)	No	Yes (How long)	No		
Removal of network access / privilege							
Outcomes /consequences/ Impact							
Additional Actions required							
SENCO involvement				BSS/Aspire involvement			
Yes (when?)		No		Yes (when?)		No	

Details of all online incidents will be recorded by the Computing lead and the relevant members of staff.

Online Safety Incident logs will be monitored half- termly by the Designated Safeguarding Lead.

Any incidents that require senior leadership team action, will be brought immediately to the attention of the Key Stage Leader, Head teacher or Designated Safeguarding Lead.

## **Appendix 5**

### **Oxford Grove Primary School Data Protection and Freedom of Information Policy September 2023**

#### **Justification**

The school will ensure that personal data is protected and kept safely and securely. It will ensure that its policy for data protection is used as the basis for collecting, storing, accessing, sharing and deleting personal data. The school will use the General Data Protection Regulations (GDPR) and Data Protection Act 2018 as the benchmark for its standard for protecting personal data.

#### **Objectives**

1. To ensure that decision makers and key people in school comply with the statutory changes in relation to GDPR and the Data Protection Act 2018.
2. To ensure that there will be regular reviews and audits of the information we hold to ensure that we fully meet the GDPR and DPA statutory requirements.
3. To document the personal data we hold, where it came from and with whom it will be shared.
4. To ensure that data collection, data handling, data storage and data disposal procedures are in line with the GDPR and cover all the rights individuals have, including how personal data is deleted and destroyed.

#### **Statements**

1. Data access request procedures will be handled within the timescales set out in the GDPR and we provide any additional information in line with the GDPR guidance.
2. The processing of personal data will be carried out on a lawful basis as required by the GDPR.
3. Where the school needs to seek consent, it will do so in a manner that meets GDPR standards.
4. Any records of consent and the management of the process for seeking consent will also meet the GDPR standard.
5. Where there is a personal data breach the procedures used to detect, report and investigate it will meet the requirements of the GDPR.
6. The systems the school puts into place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity will meet the standard set in the GDPR.
7. Data protection by design and data protection impact assessments will meet with the ICO's code of practice on privacy impact assessments as well as with the latest guidance.
8. There will be a local authority member of staff designated as the Data Protection Officer who will be given responsibility for data protection compliance.

#### **Outcomes**

The requirements of the GDPR will be met by this school as the basis for collecting, storing, accessing, sharing and deleting personal data. Data will be processed fairly lawfully and in a transparent manner. It will be used for specified, explicit and legitimate purposes in a way that is adequate, relevant and limited. It will be accurate and kept up to date and kept no longer than is necessary. Data will be processed in a manner that ensures appropriate security of the data.

#### **Review**

This document will be reviewed annually by the Head teacher, the staff and the Governing Board.

Miss N. Harvey  
Head teacher.  
To be reviewed in July 2024

## **Appendix 6**

### **Oxford Grove Primary School Artificial Intelligence Usage Guidelines Policy**

#### **Rationale**

Oxford Grove understands that Artificial Intelligence (AI) is a powerful new technology which has grown exponentially in recent times. However, due to its relative infancy, we as a school feel that more time and study into the risks and benefits of AI is required. Therefore, we have taken the decision to not use AI at Oxford Grove. We have invested in further safeguarding procedures by ensuring that websites that fall under the category of AI have been blocked from our school network.

This policy is reviewed regularly, and when such a time comes that we feel the use of AI may be of beneficial value to teaching and learning at Oxford Grove, we will consider its use within school. If and when this occurs, the following policy sets out the conditions under which AI will be used at Oxford Grove.

#### **Pupil well-being and safety:**

- a. AI systems should be used to prioritise the physical, emotional, and psychological well-being of pupils.
- b. Avoid using AI systems that may cause harm or distress to pupils.
- c. Regularly assess and monitor the impact of AI systems on pupil well-being and safety.

#### **Privacy and data protection:**

- a. Obtain informed consent from parents or legal guardians before collecting and using pupil data through AI systems.
- b. Clearly communicate to parents, pupils, and staff how pupil data will be collected, stored, and used.
- c. Implement robust data security measures to protect pupil data from unauthorized access or breaches.
- d. Anonymise pupil data whenever possible to minimize the risk of identification.

#### **Transparency and explainability:**

- a. Ensure that the functioning of AI systems used in schools is transparent and explainable.
- b. Provide accessible explanations to pupils, parents, and teachers on how AI systems make decisions or provide recommendations.
- c. Avoid using "black-box" AI systems that operate without clear explanations or insights into their decision-making processes.

#### **Avoid biases and discrimination:**

- a. Regularly audit AI systems to identify and mitigate biases or discriminatory outcomes.
- b. Ensure that AI systems do not perpetuate existing inequalities or marginalize any pupil groups.
- c. Promote diversity and inclusivity in the development and deployment of AI systems to mitigate biases.

#### **Human oversight and intervention:**

- a. AI systems should be designed to augment, rather than replace, human interaction and decision-making.
- b. Ensure that teachers and staff have the ability to intervene or override AI systems when necessary.
- c. Maintain a balance between the use of AI systems and the personalized guidance and support provided by educators.

#### **Regular monitoring and evaluation:**

- a. Continuously monitor the performance and impact of AI systems on pupil learning outcomes and well-being.
- b. Regularly evaluate the effectiveness of AI systems in achieving educational goals and identify areas for improvement.
- c. Seek feedback from pupils, parents, and teachers to understand their experiences and concerns related to AI technology.

**Ethical procurement and usage:**

- a. Select AI systems from reputable vendors who adhere to ethical guidelines and demonstrate responsible practices.
- b. Avoid using AI systems that promote excessive commercialisation or invasive advertising to pupils.
- c. Ensure that the deployment of AI systems aligns with the principles and values of the school community.

**Review of the Artificial Intelligence Usage Guidelines Policy**

The plan will be evaluated and revised annually by the Head teacher, the Business Manager with an accountability for Technology, staff and Governing Board.

Miss N. Harvey

Head teacher

To be reviewed in July 2024