

## Sunning Hill Primary School Online Safety Policy

Reviewed and Updated - September 2023

### 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
4.1- 4.4	Acceptable User Agreements documents –Pupils
5	School Data Protection 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. This Policy has been reviewed and ratified by

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

This Online Safety Policy was approved by the Governing Body on:	October 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.	October 2024
The implementation of this Online Safety Policy will be monitored by the:	Headteacher Governors DSL has responsibility for online safety, to then liaise with relevant parties to develop action plan. Computing Lead
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
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 persons / agencies should be informed:	Headteacher School DSL LADO Police <b>See Appendix 1</b>

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

## **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**

### **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 governors 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.

Where appointed, the role of the Safeguarding Governor will include:

- meetings with the headteacher/DSL
- regular monitoring of CPOMS
- ensuring robust technical support is in place to keep systems safe and secure.
- regular monitoring of filtering
- reporting to the Governing board
- attending training for online safety where appropriate

\*\* If a school is using CPOMS it is important to ensure that the lozenges are set up to be specific and appropriate, for example – PEGI, ! Tik Tok, Snapchat, Instagram etc. This will assist in collating and responding to Online Incidents.

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

The DSL will review and update the school's filtering and monitoring procedures, clearly defining roles and responsibilities within these processes. When assessing filtering and monitoring systems, governing bodies and relevant parties will consider the number of children at risk and the proportionality of costs versus safety risks. The DSL will evaluate the strength and suitability of the current cyber security measures and consider improvements where necessary.

The DSL will ensure that the school's Safeguarding/ child protection policy adequately reflects its approach to online safety, including appropriate filtering and monitoring on school devices and school networks.

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

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

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

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

### **Computing Leads**

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, where appropriate the Education for a Connected World framework is used to support the teaching of Digital Citizenship and PHSE across all year groups.

The role of the Computing Lead includes:

- providing advice for staff and signpost relevant training and resources
- liaising with relevant 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

### **School Staff**

It is essential that all staff.

- receive **annual** appropriate safeguarding and child protection training, including online safety which, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring.
- understand and acknowledge their responsibilities as outlined in this Policy.
- have read, understood and signed the Staff Acceptable Use Policy (Appendix 3)
- keep up to date with the Online Safety Policy as part of their CPD.
- will not support or promote extremist organisations, messages, or individuals.
- will not give a voice or opportunity to extremist visitors with extremist views.
- will not browse, download, or send material that is considered offensive or of an extremist nature by the school.
- have an up-to-date awareness of online matters pertinent to the children that they teach/have contact with
- report concerns and log incidents. (CPOMS)
- ensure that all digital communications with the School Community are on a professional level and only carried out using official school approved systems.
- apply this Online Safety Policy to all aspects of the Curriculum.
- share, discuss and ensure the children understand and acknowledge their responsibility to follow their age-appropriate 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 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 Headteacher at school.
- ensuring that schools are informed of any changes to guidance or any planned maintenance.
- school technical systems will be managed and reviewed annually in ways that ensure that the school meets recommended technical requirements.
- all users will have clearly defined access rights to school technical systems and devices.
- all school network users will be assigned an individual/class 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 4**)
- 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 4.1-4**)
- 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 inform 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 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.

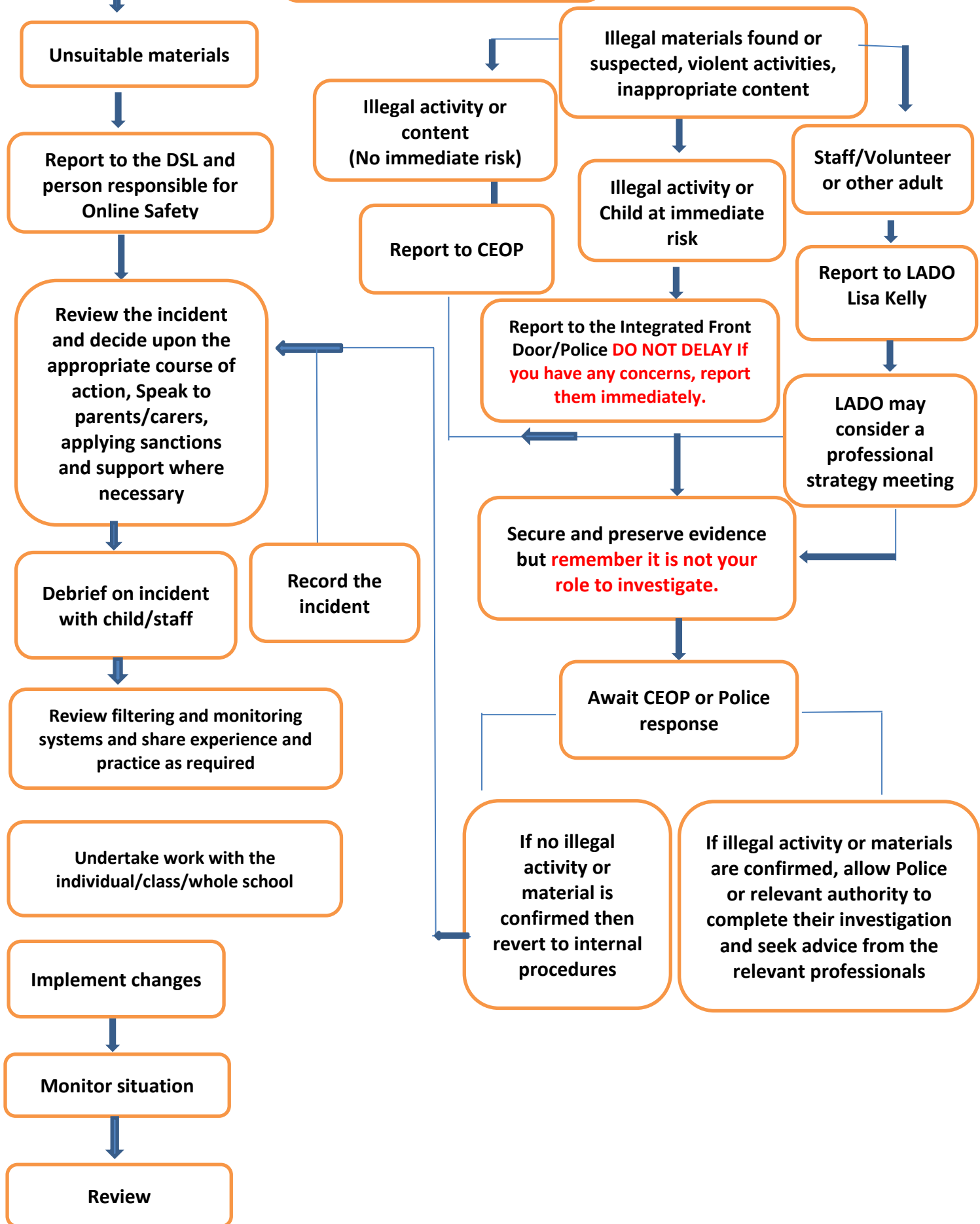
- When accessing emails out of the schools setting, staff will only be able to access their schools' emails using Microsoft Multifactor Authentication app.
- Users must immediately report to the nominated person – in accordance with the school policy, the receipt of any communication that makes them 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 (Twitter – X) 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.

 <p><b>NCA</b> Young people can report concerns about child sexual abuse and exploitation to NCA</p>	 <p><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</p>	 <p><b>ChildLine</b> A free, private and confidential service where CYP can talk about anything to a trained counsellor, online or on the phone</p>	 <p><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</p>
---	---	---	---

# Online Safety Incident Reporting





## 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



**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

Technology Standard	NOW	ASAP	AT NEXT UPDATE
<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.

**Appendix3:**

**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 and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

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

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

**Acceptable Use Policy Agreement**

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

**For my professional and personal safety:**

- I understand that the school will monitor my use of the IT systems, email and other digital communications;
- I understand that the rules set out in this agreement also apply to use of school IT systems (e.g. laptops, email etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I will not support or promote extremist organisations, messages, or individuals;
- I will not give a voice or opportunity to extremist visitors with extremist views;
- I will not browse, download, or send material that is considered offensive or of an extremist nature by the school;
- I understand that the school IT systems are primarily intended for educational use and that I will only use the systems for personal use, during breaks times and this use will be limited to appropriate websites. Restrictions are in place to stop access to facebook, gambling and other inappropriate sites. As set out in the code of conduct.
- 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.
- Staff should change passwords regularly and ensure that their passwords are strong and not used on multiple platforms or know to other users.
- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of to the DSL.
- I will be professional in my communications and actions when using school

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

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

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

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

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

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

I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school 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 a warning or suspension, dealt with through the HR disciplinary policy. Illegal activities will be reported to the Police.


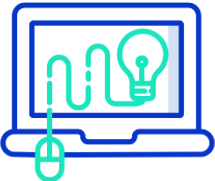


I have read and understand the above and agree to use the school IT systems (both in and out of school) and my own devices (in school and when conducting communications related to the school) within these guidelines.

Staff/Visitor/Volunteer Name

Signed

Date

# EYFS Acceptable Use Agreement

 <p><b>My Learning</b></p> <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 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 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



**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.

## Year 1 and Year 2 Acceptable Use Agreement

 <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 Signature

**Parents / Carers:**

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


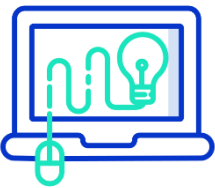


Throughout the year your child/children will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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.

## Year 3 and Year 4 Acceptable Use Agreement

 <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 Signature**

**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.

## Year 5 and Year 6 Acceptable Use Agreement

 <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>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.</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 Signature \_\_\_\_\_

**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.

# Sunning Hill Primary School

## Data Protection Policy

**COMPLETED:** K Atkinson

**APPROVED BY GOVERNORS:** February 23

**TO BE REVIEWED:** February 25

### Contents

1. Aims.....	2
2. Legislation and guidance .....	2
3. Definitions.....	2
4. The data controller .....	3
5. Roles and responsibilities.....	3
6. Data protection principles .....	5
7. Collecting personal data.....	5
8. Sharing personal data.....	6
9. Subject access requests and other rights of individuals .....	6
10. Parental requests to see the educational record.....	8
11. Photographs and videos .....	9
12. Data protection by design and default.....	9
13. Data security and storage of records .....	10
14. Disposal of records.....	10
15. Personal data breaches .....	10
16. Training.....	11
17. Monitoring arrangements .....	11
18. Links with other policies.....	11
Appendix 1: Personal data breach procedure.....	12
Appendix 2: System compliaince information.....	15



**Issue Status**

Date	Issue	Date Approved by Governors	Review date
9/11/2022	Written by Global Policing	Feb 2023	Feb 2024

## 1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

## 2. Legislation and Guidance

This policy meets the requirements of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the [GDPR](#) and the ICO's [code of practice for subject access requests](#).

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

## 3. Definitions

Term	Definition
<b>Personal data</b>	Any information relating to an identified, or identifiable, individual.  This may include the individual's: <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li><li>• Location data</li><li>• Online identifier, such as a username</li></ul> It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.
<b>Special categories of personal data</b>	Personal data, which is more sensitive and so needs more protection, including information about an individual's: <ul style="list-style-type: none"><li>• Racial or ethnic origin</li><li>• Political opinions</li><li>• Religious or philosophical beliefs</li><li>• Trade union membership</li><li>• Genetics</li><li>• Biometrics (such as fingerprints, retina, and iris patterns), where used for identification purposes</li><li>• Health – physical or mental</li><li>• Sex life or sexual orientation</li></ul>

<b>Processing</b>	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying.  Processing can be automated or manual.
<b>Data subject</b>	The identified or identifiable individual whose personal data is held or processed.
<b>Data controller</b>	A person or organisation that determines the purposes and the means of processing of personal data.
<b>Data processor</b>	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
<b>Personal data breach</b>	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

## 4. The Data Controller

**Sunning Hill Primary School** processes personal data relating to parents, pupils, staff, trustees, governors, visitors, and others, and therefore is a data controller, with the Headteacher as the person responsible.

Each school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## 5. Roles and Responsibilities

This policy applies to **all staff** employed by **Sunning Hill Primary School** and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

### 5.1 Governors

The Governing Board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

### 5.2 Data Protection Officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

The school has an independent data protection officer service supplied by Global Policing Limited. Global Policing is an organisation run by ex-senior police officers who specialise in working with schools and have vast experience of data protection matters. If you have any questions or comments, or wish to make any requests under the Regulations, you should contact them directly:

- Telephone (answerphone) 0161 212 1682
- Email [data@globalpolicing.co.uk](mailto:data@globalpolicing.co.uk)
- Website [www.globalpolicing.co.uk/data](http://www.globalpolicing.co.uk/data)

### 5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

### 5.4 All Staff

Staff are responsible for:

- Collecting, storing, and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

## 6. Data Protection Principles

The DPA is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how **Sunning Hill Primary School** aims to comply with these principles.

## 7. Collecting personal data

### 7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 ‘lawful bases’ (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering a contract
- The data needs to be processed so that the school can comply with a legal obligation

- The data needs to be processed to ensure the vital interests of the individual e.g., to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions
- The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

## 7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the [Information and Records Management Society's toolkit for schools](#)

## 8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, if personal data is sufficiently anonymised, or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

## **9. Subject Access Requests and Other Rights of Individuals**

### **9.1 Subject Access Requests**

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with?
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests must be submitted in writing, either by letter, email, or fax to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request, they must immediately forward it to the DPO.

### **9.2 Responding to Subject Access Requests**

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which considers administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

### **9.3 Recording Subject Access Requests**

A record will be kept of all Subject Access Requests and logged on the SAR database. This SAR folder and database will be securely stored on site.

A file is to be created for each subject access request and in it should be the following information: -

- Copies of the correspondence between the Trust and the data subject, and between the Trust and any other parties.
- A record of any telephone conversation used to verify the identity of the data subject
- A record of the decisions and how the Trust came to those decisions
- Copies of the information sent to the data subject. For example, if the information was anonymised, keep a copy of the anonymised version that was sent to the data subject.

The file will be kept for one year and then securely destroyed.

When the request has been completed, the record of the request will be closed in the database.

## **9.4 Other Data Protection Rights of the Individual**

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified based on public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

## **10. Parental Requests to See the Educational Record**

Requests to view educational records will be dealt with as per a data access request and we will respond within 1 month of the request.

## **11. Photographs and Videos**

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing, and promotional materials. We will clearly explain how the photograph and/or video could be used to both the parent/carer and pupil.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

## 12. Data Protection by Design and Default

We will put measures in place to show that we have integrated data protection into all our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

## 13. Data Security and Storage of Records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops, and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils, or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our IT Acceptable Use Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

## 14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.



## **15. Personal data breaches**

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1. When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

## **16. Training**

All staff and governors are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

## **17. Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed every two years.

## **18. Links with other policies**

This data protection policy is linked to our:

- Privacy Notice (Staff & Pupils)
- Subject Access Request
- Freedom of Information Policy
- School Records Management Policy
- Information Management Toolkit for Schools V5
- Safer Recruitment Policy

## Appendix 1: Personal Data Breach Procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- Data protection breaches could be caused by several factors. Some examples are:
  - Loss or theft of pupil, staff, or Governor's data and/ or equipment on which data is stored.
  - The sharing of system passwords
  - Inappropriate access controls allowing unauthorised use.
  - Equipment Failure.
  - Human Error.
  - Unforeseen circumstances such as fire or flood.
  - Hacking.
  - 'Blagging' offences where information is obtained by deception.
- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will alert the Headteacher and the chair of the Governors.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material, or non-material damage (e.g., emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned
- If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO
- The DPO will document the decision (either way) in case it is challenged later by the ICO, or an individual affected by the breach. Documented decisions are stored in the designated, protected folder on each school's system.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored in the designated, protected folder on each school's system.

## **Review and Evaluation**

The DPO and Executive Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Once the initial aftermath of the breach is over, the DPO and Executive Headteacher should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to the next available Trust Board meeting for discussion. If there is the perception that this could be a continuing risk, the Trust's risk register is to be updated accordingly and an action plan must be drawn up to address the risk. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

## **Actions to Minimise the Impact of Data Breaches**

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records): -

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the IT Manager to recall it
- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted