
# Online Safety Policy

| | |
|---|---|
| **Policy Created** | Autumn 2024 |
| **Next Review** | Autumn 2025 |

# Contents



## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**The 4 key categories of risk**

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

## 3. Roles and responsibilities

### 3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

## 3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

## 3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Computing Subject Leader(s) and Technical Support to make sure the appropriate systems and processes are in place
- Working with the Computing Subject Leader(s) and Technical Support and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

## 3.4 The Computing Subject Leader(s) and Technical Support

The Computing Subject Leader(s) and Technical Support are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly, in line with the DFE Digital and Technology Standards in Schools. (See Appendix 4)
- Conducting a full security check and monitoring the school's ICT systems on a half-termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

### 3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by informing the Headteacher, DSL or deputy DSLs, or, the Computing Subject Leader(s) and Technical Support
- Following the correct procedures by speaking with the Computing Subject Leader(s) and Technical Support if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

### 3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

### 3.8 Pupils

Pupils are expected to:

- Notify a member of staff or the headteacher of any concerns they have about things they see online
- Understand the importance of being a responsible digital citizen
- Ensure they have read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2) with their parents/carers
- Understand that school will act in response to any breach of the policy.

## 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

**All** schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## 5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or social media platforms. This policy will also be shared with parents/carers.

Online safety will also be discussed at parents' evenings where appropriate.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSLs (including deputy DSLs).

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

## 6. Cyber-bullying

### 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school's Anti-Bullying policy and the school's Behaviour policy).

### 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their individual classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school's anti-bullying policy and the school's behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in the school's behaviour policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher, or deputy headteacher(s) in their absence
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Headteacher/DSL (or deputy DSLs) to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

### 6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Devonshire Road Primary School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. Any use of these that compromises the safety of our staff/pupils/community will be treated in line with our policies on anti-bullying, safeguarding and/or behaviour.

Devonshire Road Primary School will treat any use of AI to bully pupils in line with our anti-bullying, safeguarding and behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

## 7. Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. If anybody using the school network or systems feels that there has been a safety breach in relation to online safety, they will follow the flowchart as set out in Appendix 6.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above, and, restrict access through filtering systems where appropriate.

More information is set out in the acceptable use agreements in appendices 1 to 3.

## 8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Registration time before school
- Clubs before or after school, or any other activities organised by the school

Pupils are not allowed to keep their mobile devices on their person in school, or, in their lockers/bags. Pupils must take their mobile devices to the office to be kept secure during the day.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

## 9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure (in conjunction with Bolton Schools ICT guidance). This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time

- Not sharing the device among family or friends
- Ensuring anti-virus and anti-spyware software is installed and kept up-to-date
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Computing Subject Leader(s) and Technical Support.

## 10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary and dismissal policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). This will include ensuring that staff understand their 'expectations, applicable roles and responsibilities in relation to filtering and monitoring' (KCSIE, 2024).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse others online through:
    - Abusive, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

## 12. Remote Education

In light of the COVID-19 pandemic, remote education has been utilised since March 2020 to help keep children learning. Keeping pupils and teachers safe during periods of remote education is essential. At Devonshire Road Primary School, we have adopted the use of live lessons using Microsoft Teams with enhanced safety features:

- Waiting room/lobby
- Individual logins for each child
- Presenter tools allowing control over muting and removing participants from the lesson/meeting

This list is not intended to be exhaustive.

All technology that is distributed to pupils, parents/carers and families will be risk assessed prior to use to ensure that there are no privacy issues or scope for inappropriate use; this includes ensuring that the device has relevant and up-to-date anti-virus software installed. Each family will sign a contract to agree to the terms of use. Any breach of this contract will be followed up by the senior leadership team.

During a period of remote learning, the school will maintain regular contact with parents/carers to:

- Reinforce the importance of staying safe online
- Encourage them to set age-appropriate parental controls on devices
- Direct parents to useful resources to help them keep their children safe online

We have a separate 'Remote Learning' policy, which outlines a separate user agreement for pupils and parents/carers. This can be found on our website.

## 13. Social Media

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

## 14. Monitoring arrangements

The DSL, along with the Computing Subject Leader(s) and Technical Support, will log behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Computing Subject Leader(s) and Technical Support, in conjunction with the DSL/Headteacher. At every review, the policy will be shared with the governing board. The policy will also be reviewed in light of any significant new developments in the use of technologies, new online threats, or, incidents that have taken place. Tools, such as this one here) may be used to review the approach to online safety within the school.

## 15. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Anti-bullying policy
- Staff disciplinary and dismissal policy
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

## Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS | |
|---|---|
| **Name of pupil:** | |
| **When I use the school's ICT systems (like computers) and get onto the internet in school I will:**<br>• Ask a teacher or adult if I can do so before using them<br>• Only use websites that a teacher or adult has told me or allowed me to use<br>• Tell my teacher immediately if:<br>  ○ I select a website by mistake<br>  ○ I receive messages from people I don't know<br>  ○ I find anything that may upset or harm me or my friends<br>• Use school computers for school work only<br>• Be kind to others and not upset or be rude to them<br>• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly<br>• Only use the username and password I have been given<br>• Try my hardest to remember my username and password<br>• Never share my password with anyone, including my friends<br>• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer<br>• Not use personal data on artificial intelligence tools/systems, or, use it to bully others online<br>• Save my work on the school network<br>• Check with my teacher before I print anything<br>• Log off or shut down a computer when I have finished using it<br>**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.** | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer's agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.<br>I will not post defamatory, offensive or derogatory comments about the school, its staff or any member of its community, on social media platforms.<br>I will not upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers. | |
| **Signed (parent/carer):** | **Date:** |

## Appendix 2: KS2 acceptable use agreement (pupils and parents/carers)

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS | |
|---|---|
| **Name of pupil:** | |
| **I will read and follow the rules in the acceptable use agreement policy.**<br>**When I use the school's ICT systems (like computers) and get onto the internet in school I will:**<br>• Always use the school's ICT systems and the internet responsibly and for educational purposes only<br>• Only use them when a teacher is present, or with a teacher's permission<br>• Keep my usernames and passwords safe and not share these with others<br>• Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer<br>• Tell a teacher (or sensible adult) immediately if I find any material which might upset, distress or harm me or others<br>• Always log off or shut down a computer when I've finished working on it<br>**I will not:**<br>• Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity<br>• Open any attachments in emails, or follow any links in emails, without first checking with a teacher<br>• Use any inappropriate language when communicating online, including in emails<br>• Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate<br>• Log in to the school's network using someone else's details<br>• Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision<br>• Use personal data on artificial intelligence tools/systems, or, use it to bully others online<br>**If I bring a personal mobile phone or other personal electronic device into school:**<br>• I will not use it during lessons, clubs or other activities organised by the school, without a teacher's permission<br>• I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online<br>**I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.** | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer's agreement:** I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.<br>I will not post defamatory, offensive or derogatory comments about the school, its staff or any member of its community, on social media platforms.<br>I will not upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers. | |
| **Signed (parent/carer):** | **Date:** |

## Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

**Name of staff member/governor/volunteer/visitor:**

**When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will:**

- Use the device for educational purposes only
- Maintain and update my password regularly in accordance with the guidance set out in Section 9
- Be professional in my communications online, including emails or other messaging services
- Ensure that any images taken are done so with permissions
- Maintain the full working order of the equipment, and report any faults/breaks to the Computing Subject Leader and/or Technical Support
- Only transport, hold, disclose or share personal information as outlined in the school's Information Management policy
- Work in accordance with relevant copyright laws
- Only communicate with parents/carers using official school systems
- Use artificial intelligence in-line with our artificial intelligence policy.

**When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:**

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal, extremist or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms (unless social media accounts are for the professional use of promoting the school and its ethos).
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school
- Use personal email addresses on the school ICT systems
- Upload, download or access any illegal materials
- Use any programs or software that might allow me to bypass the filtering/security systems in place.
- Use my own personal device in view of the pupils
- Use my own personal social media to negatively harm the reputation of the school
- Engage in online activity which may compromise my professional responsibilities
- Use my own personal email accounts
- Open any attachments/links which may compromise the security of the schools network systems
- Use any USB or portable storage device (unless approved by the Computing Subject Lead/Technical Support).

| ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS | |
|---|---|
| I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.<br>I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.<br>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.<br>I will let the designated safeguarding lead (DSL) and Computing Subject Lead and Technical Support know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.<br>I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.<br>I understand that if I fail to comply with the above Acceptable User Policy, this may result in disciplinary action. | |
| **Signed (staff member/governor/volunteer/visitor):** | **Date:** |

## Appendix 4: Technology Standards for Primary Schools

| Technology Standard | NOW | ASAP | AT NEXT UPDATE |
|---|---|---|---|
| **Broadband Internet Standards** | | | |
| Schools and colleges should use a full fibre connection for their broadband service | | | ✓ |
| Schools and colleges should have a backup broadband connection to ensure resilience and maintain continuity of service | | | ✓ |
| Schools and colleges should have appropriate IT security and safeguarding systems in place, under both child and data protection legislation | ✓ | | |
| **Network Switching Standards** | | | |
| The network switches should provide fast, reliable and secure connections to all users both wired and wireless | | | ✓ |
| Have a platform that can centrally manage the network switching infrastructure | | | ✓ |
| The network switches should have security features to protect users and data from unauthorised access | | | ✓ |
| Core network switches should be connected to at least one UPS to reduce the impact of outages | | | ✓ |
| **Network Cabling Standards** | | | |
| Copper cabling should be Category 6A (Cat 6A) | | | ✓ |
| Optical fibre cabling should be a minimum 16 core multi-mode OM4 | | | ✓ |
| New cabling should be installed and tested in line with the manufacturer's guidance, warranty terms, and conditions | | | ✓ |
| **Wireless Network Standards** | | | |
| Use the latest wireless network standard approved by the Wi-Fi Alliance | | | ✓ |
| Have a fully functional signal from your wireless network throughout the school or college buildings and externally where required | | | ✓ |
| Have a solution that can centrally manage the wireless network | | | ✓ |
| Install security features to stop unauthorised access | | | ✓ |
| **Cyber Security Standards** | | | |
| Protect all devices on every network with a properly configured boundary or software firewall | ✓ | | |
| Network devices should be known and recorded with their security features enabled, correctly configured and kept up-to-date | ✓ | | |

| | | | |
|---|---|---|---|
| Accounts should only have the access they require to perform their role and should be authenticated to access data and services | | ✓ | |
| You should protect accounts with access to personal or sensitive operational data and functions by multi-factor authentication | | ✓ | |
| You should use anti-malware software to protect all devices in the network, including cloud-based networks | | ✓ | |
| An administrator should check the security of all applications downloaded onto a network | | ✓ | |
| All online devices and software must be licensed for use and should be patched with the latest security updates | | ✓ | |
| You should have at least 3 backup copies of important data, on at least 2 separate devices, at least 1 must be off-site | | ✓ | |
| Your business continuity and disaster recovery plan should include a regularly tested contingency plan in response to a cyber attack | | ✓ | |
| Serious cyber-attacks should be reported | | ✓ | |
| You must conduct a Data Protection Impact Assessment by statute for personal data you hold as required by General Data Protection Regulation | ✓ | | |
| Train all staff with access to school IT networks in the basics of cyber security | | ✓<br>Within 12 months | |
| **Filtering and Monitoring Standards** | | | |
| You should identify and assign roles and responsibilities to manage your filtering and monitoring systems | ✓ | | |
| You should review your filtering and monitoring provision at least annually | ✓ | | |
| Your filtering system should block harmful and inappropriate content, without unreasonably impacting teaching and learning | ✓ | | |
| You should have effective monitoring strategies that meet the safeguarding needs of your school or college | ✓ | | |
| **Cloud Solution Standards** | | | |
| Use cloud solutions as an alternative to locally-hosted systems, including servers | | ✓ | |
| Cloud solutions must follow data protection legislation | ✓ | | |
| Cloud solutions should use ID and access management tools | | ✓ | |
| Cloud solutions should work on a range of devices and be available when needed | ✓ | | |
| Make sure that appropriate data backup provision is in place | ✓ | | |
| **Servers and Storage Standards** | | | |
| All servers and related storage platforms should continue to work if any single component or service fails | ✓ | | |
| Servers and related storage platforms must be secure and follow data protection legislation | ✓ | | |
| All servers and related storage platforms should be energy-efficient and set up to reduce power consumption, while still meeting user needs | ✓ | | |

| | | | |
|---|---|---|---|
| All server and related storage platforms should be kept and used in an appropriate physical environment | ✓ | | |

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

**Broadband Internet Standards**

The Bolton Schools ICT broadband SLA provided connection exceeds the speed required in this standard.

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

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

**Network Switching Standards**

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

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

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

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

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

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

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

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

**Network Cabling Standards**

Having your school fully rewired with new cabling is a major expense.
Most schools will have Category 5E or 6 cabling. This is suitable to provide 1Gbps connectivity to the desktop as required in the switching standards.

Category 6A cabling is capable of supporting 10Gbps which is generally only used for infrastructure links.

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

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

**Wireless Network Standards**

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

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

**Cyber Security Standards**

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

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

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

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

**Filtering and Monitoring Standards**

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

**Cloud Solution Standards**

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

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

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

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

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

**Servers and Storage Standards**

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

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

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

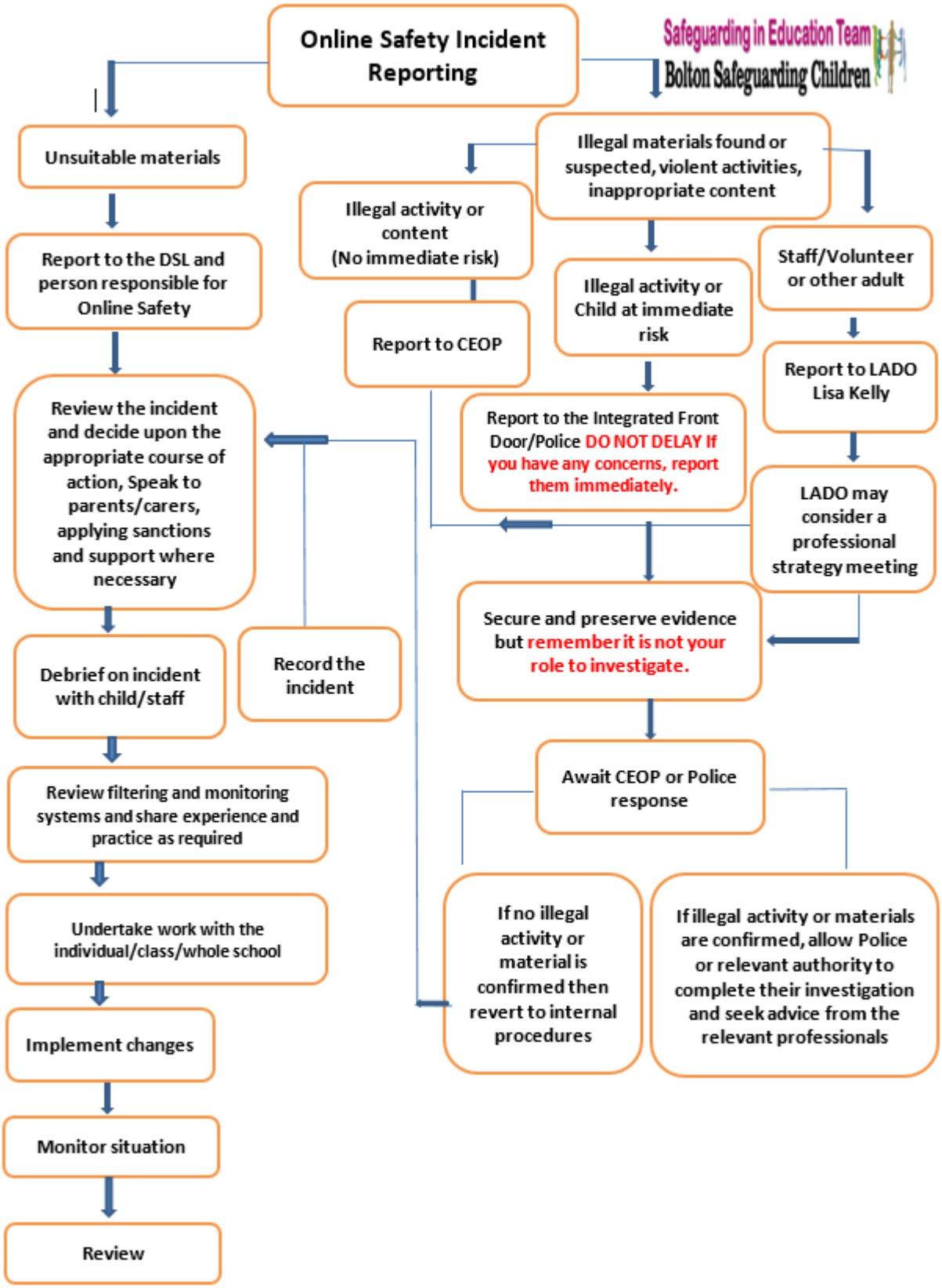
Bolton Schools ICT will keep your servers up to date and patched.

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

## Appendix 5: online safety incident report log

| ONLINE SAFETY INCIDENT LOG | | | | | |
|---|---|---|---|---|---|
| **Date** | **Where the incident took place** | **Description of the incident (including names of staff/children involved)** | **Room and Device number** | **Action taken** | **Name and signature of staff member recording the incident** |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## Appendix 6: Online Safety Incident Flowchart



## 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

### 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