Bilton CofE Junior School
Bilton Infant School
Bawnmore Community Infant School

BILTON COMMUNITY FEDERATION
ONLINE SAFETY POLICY

Federation Policy

This policy has been created considering the guidance from Warwickshire County Council and the Department of Education as per section 2 of this policy.

POLICY APPROVAL	
Statutory, recommended, or additional policy	**Recommended**
Policy review cycle	**Annual**
Policy reviewed by	**E Newton (Executive Headteacher)**
Policy review date	**June 2025**
Date of next review	**June 2026**
Date approved by Governing Body	**3rd June 2025**

1. Aims

It is our aim that our policies and procedures reflect our vision and values as a federation.

Vision: 'Empowering children to make a positive impact on the world.'

Values: Care, Honesty, Respect, Co-operation, Forgiveness and Resilience

Our schools aim 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 considers 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 Executive 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 the 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 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school 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 Executive Headteacher

The Executive Headteacher is responsible for ensuring that Heads of School understand this policy, and that they are implementing it consistently across their school.

3.3 The Head of School

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

3.4 The Designated Safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputy/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:

- Supporting the Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Head of School and 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 ICT Manager / Computing Lead to make sure the appropriate systems and processes are in place
- Working with the Head of School, ICT Manager / Computing Lead 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 on CPOMS 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 (Appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head of School, Executive 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.

3.5 The ICT Manager / Computing Lead

The ICT Manager / Computing Lead is 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
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis and reported to the Head of School. All schools use the Warwickshire Digital Monitoring team who immediately inform the school of any security or monitoring concerns.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged on CPOMS 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.

3.6 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 2), and ensuring that pupils follow the school's terms on acceptable use (Appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware that any incidents where the systems or processes fail must be reported directly to the DSL on site.
- Following the correct procedures by speaking to the DSL in the first instance and then the ICT Manager / Computing Lead 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 on CPOMS 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.

3.7 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Head of School 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 (Appendix 1)

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
- Parent resource sheet – Childnet

3.8 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 2).

4. Educating pupils about online safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary 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 junior 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. This policy will also be shared with parents/carers.
Online safety will also be covered during parents' evenings.
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 Head of School and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the Head of School.

6. Filtering and monitoring

Considering the schools responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies should ensure the school has appropriate filters and monitoring systems in place and **regularly review their effectiveness**.

They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.

Governing bodies should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks.

The appropriateness of any filters and monitoring systems has been agreed by the schools and is informed in part, by the risk assessment required by the Prevent Duty.

To meet this duty, in reference to the Department for Education filtering and monitoring standards (**see Appendix 4**) our schools will endeavour to:

• identify and assign roles and responsibilities to manage filtering and monitoring systems.
• review filtering and monitoring provision at least annually.
• block harmful and inappropriate content without unreasonably impacting teaching and learning.
• have effective monitoring strategies in place that meet their safeguarding needs

Governing bodies and proprietors will review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

The DSL logs behaviour and safeguarding issues related to online safety, using the CPOMS system.

7. Cyber-bullying

7.1 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.

7.2 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, in an age appropriate manner, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

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 12 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 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.

7.3 Examining electronic devices

The Head of School, and any member of staff authorised to do so by the Head of School, 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 Head of School.
- 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 DSL / Head of School 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.

7.4 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.

Bilton Community Federation 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. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

Bilton Community Federation will treat any use of AI to bully pupils in line with our behaviour policy. 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/trust.

8. 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 (Appendix 1 & 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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 Appendix 1 & 2.

9. Pupils using mobile devices in school

Mobile devices are not allowed to be brought in by pupils at either infant school.

Mobile devices are allowed to be brought in to the Junior School, in line with the Home School Agreement, but should be handed straight in to the school office and should not be used on site at any time.

Any breach of the Home School Agreement by a pupil may trigger disciplinary action in line with the

school behaviour policy, which may result in the confiscation of their device.

In exceptional circumstance a mobile device may be needed in school, for example where medical needs require this. In such instances a risk assessment and personal agreement between school, child and parent will be drawn up.

10. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. 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
- Installing anti-virus and anti-spyware software
- 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 either the ICT Manager / Computing Lead or the Head of School.

11. 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 policies on behaviour and safeguarding. 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 procedures.

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.

12. 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.

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 their peers online through:
    - Abusive, threatening, 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 deputies 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 BCF Safeguarding policy.

12.1 Pupil Training

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate training on safeguarding issues such as cyberbullying and the risks of online radicalisation.

This policy will be reviewed every year by the Executive Headteacher. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- BCF Safeguarding policy
- School Behaviour policy
- BCF Staff Disciplinary Procedures
- BCF Data Protection Policy
- BCF Complaints Policy & Procedure
- BCF Staff and Governor Use of Social Networking and Internet Sites

Appendix 1 School's Acceptable Use Policies:

Appendix 1a: Bilton Infant School Children's Acceptable Use Policy

Pupil Acceptable Use Policy

RESPECT

I am **responsible** using online equipment.

I make sure I have finished eating or drinking before I **enjoy** using online equipment.

I keep my personal information **safe** and **secure**, including passwords to devices.

I ask **permission** before going online.

I **end** what I am doing when I am asked or if I see something that gives me a worried feeling.

I **choose** games and activities I play **carefully**, with help from adults, so that I keep myself safe.

I **tell** a trusted adult if I get a worried feeling and keep telling until the worried feeling stops.

I agree to follow these rules set out above.
I know that if I break any of these rules my parents / carers may be told.

Name _____

Date _____ Class _____

This document has been developed in consultation with our Online Safety Rangers, Staff, Parents and Governors to help you understand the rules of using any online devices. You should always follow the rules set out in this policy because these rules will help keep you safe online both in school and at home.

Appendix 1b: Bawnmore Community Infant School Children's Acceptable Use Policy

Bawnmore Community Infant School

Rules for staying safe on the computers

- We will ALWAYS ask an adult first if we can go on the internet or a computer
- We will tell an adult if anything strange comes up on the screen
- We will ALWAYS ask an adult if we can change the activity we are using
- We will not give people our phone number or address
- We will not send photographs of ourselves to people that we do not know
- We will take care of the computers and always use them properly

Child signature.....

Parent/carer signature .....

Date.....

Bilton C of E Junior School Pupil Acceptable Usage Policy

- I will only access computing equipment with permission.
- I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
- I will keep my username and password secure.
- I will never share mine or others personal information, such as telephone numbers, addresses and names or photographs.
- I will use my own username and password to access the school equipment.
- I'm aware school monitors my online use.
- I will respect computing equipment.
- I will use all communication tools such as emails carefully.

I understand this agreement and understand my parents /carers will be notified if I break the rules.

My Name……

Child signature……

Class……

Parent / Carer Signature……

Date……

Appendix 2: 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 not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way that could harm the school's reputation • Access social networking sites or chat rooms, other than those used as part of the school's communication processes, such as school Facebook page. • 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 without checking with teachers first • 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	
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. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. 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. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: Online Safety Training Needs Audit

Online Safety Training Needs Audit	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: Filtering and monitoring standards for schools and colleges

Schools and colleges have a statutory responsibility to keep children and young people safe online as well as offline. Governing bodies and proprietors should make sure their school or college has appropriate filtering and monitoring systems in place, as detailed in the statutory guidance, Keeping children safe in education.

Filtering is preventative. It refers to solutions that protect users from accessing illegal, inappropriate and potentially harmful content online. It does this by identifying and blocking specific web links and web content in the form of text, images, audio and video.

Monitoring is reactive. It refers to solutions that monitor what users are doing on devices and, in some cases, records this activity. Monitoring can be manual, for example, teachers viewing screens as they walk around a classroom. Technical monitoring solutions rely on software applied to a device that views a user's activity. Reports or alerts are generated based on illegal, inappropriate, or potentially harmful activities, including bullying. Monitoring solutions do not block users from seeing or doing anything.

The job titles in these standards may not fit your educational setting, but the responsibilities described should be applied to the most relevant person.

These standards help school and college leaders, designated safeguarding leads and IT support understand how to work together to make sure they can effectively safeguard their students and staff.

We want to know how you're meeting these standards, what barriers you might face and what could help. Share your views in our public consultation on narrowing the digital divide in schools and colleges.

Identify and assign roles and responsibilities to manage your filtering and monitoring systems

Why this standard is important
Schools and colleges should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding students and staff from illegal, inappropriate and potentially harmful online material.
Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that your designated safeguarding lead (DSL) and IT support work together, using their professional expertise to make informed decisions. Governors and your senior leadership team (SLT) should provide support as required.

How to meet the standard
Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.
To do this, they should identify and assign:

- a member of the SLT and a governor, to be responsible for ensuring these standards are met
- the roles and responsibilities of staff and third parties, for example, in-house or third-party IT support

There may not be full-time staff for each of these roles. Some responsibilities may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible and it must be possible to make prompt changes to your provision.

Technical requirements to meet the standard
The SLT is responsible for:

- buying filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Senior leaders should work closely with governors or proprietors, the DSL and IT support in all aspects of filtering and monitoring. Your IT support may be in-house or a third-party service provider.

Day-to-day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT support to be effective.

Your DSL should lead on safeguarding and online safety as detailed in the Keeping children safe in education statutory guidance. This should include, among other duties:

- checking relevant reports
- responding to safeguarding concerns identified by filtering and monitoring
- providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly

Your DSL should take any necessary action in line with Keeping children safe in education and your existing safeguarding policies. Make sure all users, parents and carers are aware of your policy.
Your in-house or third-party IT support have technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or system checks

Your in-house or third-party IT support should work with your SLT and DSL to:

- help buy systems
- identify risk
- carry out reviews
- carry out checks

When to meet the standard
You should already be meeting this standard.

Review your filtering and monitoring provision at least annually

Why this standard is important
For filtering and monitoring to be effective it should meet the needs of your students and staff. It should reflect your specific use of technology while minimising potential harms.
To understand and evaluate the changing needs and potential risks of your school or college, you should review your filtering and monitoring provision at least once every academic year.
The review process should identify additional filtering and monitoring checks that are needed. This will give governing bodies and proprietors assurance that systems are working effectively and meeting safeguarding obligations.

How to meet the standard
Governing bodies and proprietors have overall strategic responsibility for meeting this standard. They should make sure that filtering and monitoring provision is reviewed at least once every academic year. This can be part of a wider online safety review.
The review should be conducted by members of the senior leadership team, the designated safeguarding lead, and IT support. It should also involve the responsible governor. You should record the results of the online safety review and make it available to anyone who is entitled to inspect that information.

Technical requirements to meet the standard
A review of filtering and monitoring should be carried out to identify your current provision, any gaps, and your students' and staff's specific needs.

You need to understand:

- how your students' risk profile could inform your approach to filtering and monitoring, considering things such as their age, if they have any special education needs and disabilities (SEND) and whether they have English as an additional language (EAL)
- what your filtering system currently blocks or allows
- technical limitations, for example, whether your solution can filter real time content
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports or serious incidents
- the digital resilience of your students
- teaching requirements, for example, your relationships, sex and health education (RHSE) and personal, social, health and economic (PSHE) curriculum
- how your school or college uses technology, including bring your own device (BYOD) for students and staff, and generative AI tools
- what related safeguarding or technology policies are in place
- what checks are currently taking place and how resulting actions are handled
- any technical set-up recommendations to make sure the system works effectively

To make your filtering and monitoring provision effective, your review should inform:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- staff training
- curriculum and learning opportunities
- how often and what is checked
- monitoring strategies
- procurement decisions

Following system or equipment changes, you should seek assurance that all filtering and monitoring solutions will continue to work on all school-managed devices.

The review should take place, as a minimum, once every academic year or when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD
- new technology is introduced, such as new devices
- major software updates occur
- there are changes to the technical configuration of the network and devices

If your review identifies any risks or issues with filtering and monitoring on devices, you will need to investigate. Try to resolve the issue by reviewing your filtering and monitoring provision or adjusting your device settings. Always consider your student risk profile when deciding whether to continue using the devices in question.

There are links and advice to further guidance in the reviewing online safety section of Keeping children safe in education.

Checks to your filtering provision need to be completed and recorded as part of your filtering and monitoring review process. How often the checks take place should be based on your school or college context, the risks highlighted in your filtering and monitoring review, and any other risk assessments. Checks should be made from both a safeguarding and IT perspective.

When checking filtering and monitoring systems you should make sure that the system setup has not changed or been deactivated. This should include checking:

- school or college owned devices and services – these are all internet connected devices managed by the school or college, even if they are taken home, and include laptops, tablets and audiovisual equipment
- locations and different sites if there are buildings, schools or colleges on different premises
- that user group accounts are filtering the correct content for students, staff and guests

You should keep a log of your checks so they can be reviewed. You should record:

- when the check took place
- who did the check
- what they tested or checked

- resulting actions

You should make sure that:
- all staff know how to report and record concerns
- filtering and monitoring systems work on new devices and services before distributing them
- inappropriate content that you choose to block is reviewed and updated in line with changes to guidance and safeguarding risks

You can use South West Grid for Learning's (SWGfL) testing tool to check that, as a minimum, your filtering system is blocking access to:
- illegal child abuse material
- unlawful terrorist content
- adult content

When to meet the standard
You should already be meeting this standard.

Filtering systems should block harmful and inappropriate content without unreasonably impacting teaching and learning

Why this standard is important
An active and well-managed filtering system is an important part of providing a safe environment for students to learn.
No filtering system can be 100% effective. You need to understand:
- your filtering system's coverage
- any limitations

You should mitigate against these limitations to minimise harm and meet your statutory duties in the filtering and monitoring section of Keeping children safe in education and the Prevent duty guidance: England and Wales (2023)
An effective filtering system needs to block internet access to harmful sites and inappropriate content. It should not:
- unreasonably impact teaching and learning or school or college administration
- restrict students from learning how to assess and manage risk themselves
-

How to meet the standard
Governing bodies and proprietors need to support the senior leadership team (SLT) to procure and set up systems which meet this standard and satisfy your school or college risk profile. This may need to be different for different user types, year groups and subjects.

Your filtering system should not have a blanket filtering profile for all users. As a minimum, student and staff profiles should be in place to provide differing levels of access to online content.

Filtering system management requires specialist knowledge from both safeguarding and IT support to be effective. You may need to ask your filtering provider for system specific training and support.

Technical requirements to meet the standard
The Internet Watch Foundation (IWF) and Counter-Terrorism Internet Referral Unit (CTIRU) provide lists of illegal websites that filtering providers can block as part of their service, known as blocklists. Schools and colleges must make sure these blocklists are included with their filtering solutions. Your school or college should not be able to disable these blocklists or remove items from them.
Also make sure that your filtering provider is:
- a member of IWF
- signed up to CTIRU
- regularly updating blocklists based on information from IWF and CTIRU

Some schools and colleges may want to block additional, inappropriate content that their filtering system does not automatically block. Your system should allow you to add this content locally. Any additions should not disrupt or affect teaching and learning.

Your filtering system should be active, up to date and applied to all:

- school or college-managed devices, including those taken off-site
- unmanaged devices under a bring your own device (BYOD) scheme
- guests who have access to the school internet

Devices that are not school or college-managed, should be on a separate virtual network. Check with your provider to find out whether your filtering system:

- identifies and appropriately filters all internet feeds, including any backup connections and portable wifi devices
- is appropriate for the age and ability of the users
- is suitable for educational settings
- identifies multilingual web content, images, common misspellings and abbreviations
- provides alerts when web content of concern has been blocked
- blocks technologies and techniques that allow users to get around the filtering, such as VPNs, proxy services and end-to-end encryption methods

If you are unsure about how to do this, ask your IT support or filtering provider to block these technologies at a system level. Also ask them to make sure that networks and clients are appropriately configured, this covers everything from firewalls and browsers to operating systems and software.

Mobile and app content is often presented in a different way to web browser content. If your users access content in this way, you should get confirmation from your provider as to whether they can provide filtering on mobile or app technologies. A technical monitoring system should be applied to devices using mobile or app content to reduce the risk of harm.

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the SLT or the designated safeguarding lead.
Your filtering systems should allow you to identify, as a minimum:

- device name or ID, IP address, and where possible, the individual
- the time and date of attempted access
- the search term or content being blocked
-

Schools and colleges will need to conduct their own data protection impact assessments (DPIAs) and review the privacy notices of third-party providers. A DPIA template is available from the Information Commissioner's Office (ICO).

The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

Search engines used should have safe search enabled by default, or use a child-friendly search engine, to provide an additional level of protection for your users in addition to the filtering service. Make sure that:

- your safe search engine is locked into your chosen browser and cannot be changed
- users cannot download additional browsers or unauthorised plugins

If the filtering provision is procured with a broadband service, ask your broadband provider how it meets these requirements.

All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They should report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material
- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material
-

The UK Safer Internet Centre has guidance on establishing appropriate filtering.

Dependencies to the standard
Check that you meet:

- broadband internet standards
- cyber security standards

When to meet the standard
You should already be meeting this standard.

Have effective monitoring strategies that meet the safeguarding needs of your school or college

Why this standard is important
Monitoring user activity on school and college devices is an important part of providing a safe environment for students and staff. Unlike filtering, it does not stop users from accessing material through internet searches or software.

Monitoring allows you to review user activity on school and college devices. There are both technical and manual solutions. Which solution your school or college uses will depend on your educational setting, including:

- student age
- student risk profile
- whether screens are easy to see
- number of devices in use
- whether devices are used off-site, for example, at home

For monitoring to be effective it must pick up incidents that are of concern urgently, usually through alerts or observations, allowing you to take prompt action and record the outcome.

How to meet the standard
All staff should conduct a level of in-person monitoring if they are in a room with students on devices, as part of wider classroom supervision. Some schools and colleges may decide to have additional technical monitoring solutions in place to reduce any risks identified during the review.

The designated safeguarding lead (DSL) is responsible for any safeguarding and child protection matters that are identified through monitoring.

The management of technical monitoring systems requires the specialist knowledge of both safeguarding and IT support to be effective. Training should be provided to make sure their knowledge is current. You may need to ask your technical monitoring system provider for system-specific training and support.

Technical requirements to meet the standard
Your monitoring plan should include how you will monitor students when using school-managed devices connected to the internet. This could include:

- device monitoring using device management software
- in-person monitoring in the classroom
- network monitoring using log files of internet traffic and web access

As a minimum, your monitoring plan should include weekly monitoring reports highlighting incidents. It should also include immediate reports when an incident is classed as high-risk, for example, those of a malicious, technical or safeguarding nature.

Make sure that everyone using your school's network knows that filtering and monitoring processes are in place. Technical monitoring systems should also notify users that the device is being monitored. This could be a message each time they log in.

Your monitoring plan should include how you communicate with staff about accepted ways of responding to incidents, including:

- how to deal with incidents
- who should lead on any actions
- when incidents should be acted on, in line with your school's policy – read the first standard about filtering and monitoring roles and responsibilities to help with this

There should be a documented process for recording incidents that includes what action was taken and the outcomes. This will help you to understand the effectiveness of your filtering and monitoring plan.

The UK Safer Internet Centre has guidance for schools and colleges on establishing appropriate monitoring.
Device monitoring can be managed by in-house or third-party IT support, who need to:

- make sure monitoring systems are working as expected both on-site and off-site
- provide reporting on student device activity
- receive safeguarding training including online safety
- record and report safeguarding concerns to the DSL

Make sure that:

- monitoring data is received in a format that your staff can understand
- users are identifiable to the school or college, so concerns can be traced back to an individual, including guest accounts where possible

If mobile or app technologies are used then you should apply a technical monitoring system to the devices, as your filtering system might not pick up mobile or app content.

In the online safety section of Keeping children safe in education there is guidance on the 4 areas of risk that users may experience when online. Your monitoring provision should identify and alert you to behaviours associated with them.

Technical monitoring systems do not stop unsafe activities on a device or online. Staff should:

- provide effective supervision
- take steps to maintain awareness of how devices are being used by students
- report any safeguarding concerns to the DSL
-

School and college monitoring procedures need to be reflected in your acceptable use policy (AUP). Add them to relevant online safety, safeguarding and organisational policies, such as privacy notices.

Schools and colleges that have a technical monitoring system will need to conduct their own data protection impact assessment (DPIA) and review the privacy notices of third-party providers. Visit the Information Commissioners Office website to download a DPIA template.

The DfE data protection toolkit includes guidance on privacy notices and DPIAs.

Dependencies to the standard
Check that you meet:

- cyber security standards

When to meet the standard
You should already be meeting this standard.

Appendix 5: BCF Online Safety Policy on a Page

BCF Online Safety Policy on a Page

4 Categories of Risk:

- Content – what children could be exposed to;
- Contact – harmful online interaction;
- Conduct – own personal behaviour that increases likelihood of harm;
- Commerce – the risks of online gambling, purchases and effect of inappropriate advertising.

Responsibilities:

- Governing Board – responsible for monitoring the policy and its implementation.
- Executive Headteacher – responsible for ensuring Heads of School understand and implement the policy.
- Heads of School – the day to day implementation of the policy and procedures that support the policy.
- ICT Manager / Computing Lead – managing and monitoring the school systems to support the implementation of this policy.
- Staff – maintain and understand the policy and support the implementation of it.
- Parents/Carers – notify school of any concerns or queries regarding the policy and ensure their child knows and understand the expectations when using the school's ICT systems and internet.

Education:
The schools will all follow the statutory requirements around the computing programmes of study in order to meet the expectations of the curriculum and at each key stage.

Filtering & Monitoring:
The schools will filter and monitor the online environment within school in order to maintain a safe place for learning and minimise the risk of exposure to the 4 categories above. This will be done in line with the Department for Education standards.

Cyber-bullying:
The schools will, as part of their curriculum delivery, help children understand what cyber-bullying is and what they can do if they become aware of it happening to themselves or others.

Acceptable use of the Internet:
All pupils, parents, staff, volunteers and governors are expected to sign and adhere to the acceptable use agreement of the school's ICT systems and internet.

Staff Devices:
Staff will take appropriate steps to ensure their devices remain secure as laid out in full within the policy.

Issues of Misuse:
Where potential misuse is identified the school will respond in line with their behaviour and safeguarding policies.