



Burford School and Nursery

'Enjoy, Achieve, Succeed Together'

ONLINE SAFETY POLICY

Date policy adopted by Governing Body: September 2026	Date of next review: September 2027
This policy will be subject to review every year by the Governing Body or more frequently in the light of changes in legislation	

1. Aims

Our school aims to:

- Have robust processes in place to ensure the Online Safety of children, staff, volunteers and governors
- 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 any concerns, 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, racism, misogyny, self-harm, suicide, antisemitism, radicalization, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **Contact** – being subjected to harmful online interaction with other users or generative AI (artificial intelligence) applications that simulate this, 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** – online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images including those generated by AI (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography) and online bullying
- **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) statutory safeguarding guidance, [Keeping Children Safe in Education 2026](#), and its advice for schools on:

[Teaching Online Safety in schools](#)

[Preventing and tackling bullying](#) and [cyberbullying: 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](#), the [Equality Act 2010](#) and the [Education Act 2011](#).

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 Safeguarding Governor will oversee the use of Online Safety in school.

All governors will:

- ensure that they have read and understand this policy
- agree and adhere to the terms on acceptable use of the school's devices and the internet (Appendix 1)
- ensure that Online Safety is reflected as required in all relevant policies
- ensure that Online Safety is considered when planning:
 - the curriculum
 - any teacher training
 - the role and responsibilities of the designated safeguarding lead (and deputies)
 - any parental engagement
- ensure that, where necessary, teaching about safeguarding, including Online Safety, is adapted by the school for vulnerable children, victims of abuse and some children with SEND 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 Headteacher alongside the IT support team

The Headteacher, with support from the IT support team (MET), is responsible for:

- ensuring appropriate levels of security protection procedures, such as filtering and monitoring systems, are reviewed and updated on a regular basis to assess effectiveness and ensure children 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 devices 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 devices on a monthly basis
- ensuring access to potentially dangerous sites is blocked, including any generative AI applications and, where possible, preventing the downloading of potentially dangerous files
- ensuring that staff devices are installed with anti-virus and anti-spyware software
- ensuring hard drives are encrypted on school laptops – 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
- ensuring that any Online Safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- ensuring that online searches are conducted as part of any due diligence checks during the recruitment process and that shortlisted candidates are made aware of this process in advance.

3.4 The designated safeguarding lead (DSL)

Details of the school's DSL and Deputy DSLs are set out in our Child Protection and Safeguarding Policy.

The DSL takes lead responsibility for Online Safety in school, in particular:

- supporting in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- working with staff, as necessary, to address any Online Safety concerns, issues or incidents
- managing all Online Safety concerns, issues and incidents in line with the school's Child Protection and Safeguarding Policy
- understanding the schools' filtering and monitoring systems and processes
- ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with KCSiE
- updating and delivering staff/governor training on Online Safety
- liaising with other agencies and/or external services if necessary
- providing regular reports on Online Safety in school to the governing board as part of the safeguarding review.

3.5 The Computing Lead

The Computing Lead is responsible for:

- ensuring that the Computing curriculum at Burford School is relevant and up to date, as well as monitoring the quality of its implementation
- ensuring that Online Safety materials are relevant and in line with the statutory guidance
- maintaining communication with the IT support team to ensure that devices are up to date with necessary software for implementing the curriculum effectively.

3.6 All staff and volunteers

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

- implementing this policy consistently
- ensuring that any Online Safety incidents are logged on CPOMS and dealt with appropriately in line with this policy (members of staff only)

- modelling appropriate use of devices inside and outside of school and ensuring that children follow the school's Internet Code of Conduct agreement (Appendix 1)
- ensuring that any incidents of cyberbullying are dealt with appropriately in line with the school's 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'
- where relevant, checking that all online resources used in lessons are safe and appropriate for the cohort
- when instructing the children to use devices, ensure that they are adequately supervised at all times.
- ensuring that the safe boxes containing mobile devices belonging to the children are locked at the beginning of the school day (Years 5 and 6 staff only) and that no **smart** devices are brought onto school site.

3.7 Parents

Parents are expected to:

- notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- ensure that their child has read, understood and agreed to the terms on acceptable use of the school's devices and internet (Appendix 1).

Parents can seek further guidance on keeping children safe online from the organisations and websites listed on the Burford School website using the link below:

<https://www.burfordschool.co.uk/online-safety/>

3.8 Visitors and members of the community

Visitors and members of the community who use the school's devices 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 set out on MET Central.

4. Educating children about Online Safety

Children will be taught about Online Safety as part of the curriculum.

In **Key Stage 1**, children 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.

Children in **Key Stage 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**, children 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 subjects where relevant.

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

5. Educating parents about Online Safety

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

If parents have any queries or concerns in relation to Online Safety, these should be raised in the first instance with the Headteacher or the DSL Deputies.

6. Cyberbullying

6.1 Definition

Cyberbullying takes place via mobile phone or online, such as through email, social networks, instant messenger or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group.

6.2 Preventing and addressing cyberbullying

To help prevent cyberbullying, we will ensure that children understand what it is and what to do if they become aware of it happening to them or others. We will ensure that children 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 cyberbullying with children, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying.

All staff and governors receive training on cyberbullying, its impact and ways to support children, as part of safeguarding training (see section 11 for more detail).

In relation to a specific incident of cyberbullying, the school will follow the processes set out in the school's Behaviour Policy. Where illegal, inappropriate or harmful material has been spread among children, the school will use all reasonable endeavours to ensure the incident is dealt with swiftly.

If illegal material is involved, the DSL will work with any necessary external services and report the incident to the local authority.

7. Internet Code of Practice Agreement

All children are expected to complete a Google Form agreement regarding the acceptable use of the school's devices and the internet. 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.

The Headteacher will monitor the websites visited by children, staff and governors to ensure they comply with the above.

A link to the Internet Code of Practice agreement is in Appendix 1.

8. Children using mobile devices in school

Only children in Years 5 and 6 may bring mobile devices into school, but are not permitted to use them during the school day or in before- or after-school activities organised by the school. Smart watches are not permitted in school at any time.

From September 2026, pupils (Years 5 and 6) will no longer be permitted to bring smart devices to school. Mobile devices brought into school should only have basic communication functionalities and should not be able to take photos or connect to the internet.

All mobile devices must be kept in the lockable safe boxes (situated in the Year 5 and 6 classrooms) during the day and must be taken home at the end of each day.

Any breach of the acceptable use agreement by a child 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. 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)
- making sure the device locks if left inactive for a period of time
- not sharing the device among family or friends
- keeping operating systems up to date – always allow the latest updates to be installed when prompted.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out on MET Central.

Work devices must be used solely for work activities.

10. How the school will respond to issues of misuse

Where a child misuses the school's devices 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 devices 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/staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will report any incidents which involve illegal activity or content to the police and consider whether this is necessary for otherwise serious incidents.

11. Training

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

All staff members and governors 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, staff meetings and the completion of online e-learning modules).

By way of this training, all staff and governors 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, harassing, and discriminatory messages
 - non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around social media, including those created by AI.
 - 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 to:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure children can recognise dangers and risks in online activity and can weigh up the risks
- develop the ability to influence children to make the healthiest long-term choices and keep them safe from harm in the short term
- become aware of the benefits and risks of the use of Artificial Intelligence (AI) services
- understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

The DSL and Deputy DSLs will undertake specific 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. More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

12. Monitoring arrangements

The DSL will monitor behaviour and safeguarding issues related to Online Safety on CPOMS.

This policy will be reviewed every year by the Headteacher. At every review, the policy will be shared with the governors.

13. Links with other policies

This Online Safety policy is linked to our:

Child Protection Policy

Behaviour Policy

Anti-Bullying Policy

Staff Code of Conduct

MET Use of AI policy

MET Staff Acceptable Use of ICT Systems Policy

Staff Disciplinary Procedures

Data Protection Policy

Pupil Privacy Notice

Staff Privacy Notice

Complaints Procedure

Appendix 1: Internet Code of Practice form

Use the following link to access the Internet Code of Practice form that is completed by all new pupils to Burford School:

<https://forms.gle/yXPoh9YsDzWrnMdaA>