Pathway Trust

Online Safety Policy

Policy effective from	1 September 2026
Policy owner	Director of Inclusion
Policy applies to	Berrow Church Primary School Burnham-on-Sea Infant School Castle Batch Primary School Charfield Primary School Cherry Garden Primary School Downend School East Huntspill Primary School Lyde Green Primary School Mangotsfield School Marlwood School Pawlett Primary School Priory Community School Severn Beach Primary School St Andrew's Church Junior School St Anne's Church Primary School The Castle School The King Alfred School Tortworth Primary School West Huntspill Primary School Worle Community School Pathway Partnership Teams
Policy changes since last version	New policy

1. Rationale

1.1. Being online is an integral part of children and young people's lives. Social media, online games, websites and apps can be accessed through mobile phones, computers, laptops and tablets – all of which form a part of children and young people's online world.

1.2. The internet and online technology provides new opportunities for young people's learning and growth, but it can also expose them to new types of risks. Online safety should form a fundamental part of schools' safeguarding and child protection measures. Our schools aim to:

- Have robust processes in place to ensure the online safety of pupils, staff and volunteers.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Approach

2.1. New technologies have become integral to the lives of children and young people in today's society, both within their academic lives and also in their lives away from schools. We want young people to be able to fully utilise the benefits offered by IT while doing so in a safe manner.

2.2. Online messaging, social networking and mobile technology effectively mean that children can always be 'online'. Their social lives, and therefore their emotional development, are bound up in the use of these technologies. Latest e-safety guidance states that the breadth of e-safety issues can be categorised into four areas of risk:

- Content: being exposed to illegal, inappropriate or harmful material.
- Contact: being subjected to harmful online interaction with other users.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.
- Commerce - risks such as online gambling, inappropriate advertising, phishing and/or financial scam.

2.3. The purpose of this policy is to ensure that trust's schools are kept aware of the risks as well as the benefits of technology and how to manage these risks and keep themselves and others safe. It details the measures that the schools have put in place to support this as well as the rules and restrictions around the use of IT and other technology across the trust.

3. Legislation and guidance

3.1. This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying, and searching, screening and confiscation.

3.2. It also refers to the Department'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.

3.3. In addition, it reflects the Education Act 2011, which gives teachers 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.

3.4. The policy also takes into account the National Curriculum computing programmes of study. This policy complies with our funding agreement and articles of association.

4. Roles and responsibilities

4.1. The Board of Trustees

The trustees have overall responsibility for monitoring this policy and ensuring systems are in place for holding the Headteachers to account for its implementation.

4.2. Headteachers

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being adhered to consistently throughout the school. The Headteacher or online safety lead in school will coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding leads (DSL).

The Headteacher is responsible for ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the trust's Behaviour Policy.

4.3. Designated Safeguarding Leads

Details of the school's designated safeguarding leads (DSL) are set out in the trust's Child Protection and Safeguarding Policy.

The DSL takes lead responsibility for online safety in school, in some cases supported by an online safety lead and the safeguarding team, in particular:

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the Headteacher, Head of IT and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.

- Ensuring that any incidents of cyberbullying 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.
- Ensuring that any online safety incidents are monitored and logged and dealt with appropriately in line with this policy.

This list is not intended to be exhaustive.

4.4. **Head of IT**

The Head of IT is responsible for:

- Working across the trust to ensure that appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at the school, including terrorist and extremist material.
- Ensuring that where breaches are reported they are investigated and appropriately resolved.

4.5. **Staff and volunteers**

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

- Understanding and adhering to this policy.
- Agreeing and adhering to the terms on acceptable use of the school and trust IT systems.
- Working with the DSL to ensure that any online safety incidents are logged 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's behaviour procedures.

This list is not intended to be exhaustive.

4.6. **Parents/Carers**

Parents/Carers are expected to:

- Notify a senior member of staff or the Headteacher of any concerns or queries regarding this policy.
- Understand that their child is expected to use the school's IT systems responsibly.

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

- What are the issues? - UK Safer Internet Centre.

- Help and Advice for Parents and Carers
- Parents and Carers resource sheet | Childnet

4.7. **Visitors and members of the community**

Visitors and members of the community who use the school and trust IT 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.

5. Educating pupils about online safety

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

5.2. In Key Stage 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.

5.3. Pupils 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.

5.4. In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

5.5. Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns.

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

5.7. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

6. Educating parents/carers about online safety

6.1. 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.

6.2. Online safety may also be covered during parents'/carers' evenings/workshops.

6.3. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the Headteacher.

7. Cyber-bullying

7.1. 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 one person or group by another person or group, where the relationship involves an imbalance of power.

7.2. Prevention 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. Teachers are encouraged to find opportunities to use aspects of the curriculum to cover cyberbullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All school staff receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training. The school also sends information/leaflets on cyber-bullying to parents/ carers so that 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 behaviour policy. Cyber-bullying will be dealt with in the same way as in-person bullying.

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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

7.3. Examining electronic devices

Staff working in schools have the specific power under the Education and Inspections Act 2006 and Education Act 2011 to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and

other tablet devices, where they believe there is a 'good reason' to do so. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the trust's complaints procedure.

8. Acceptable use of the internet in schools

8.1. All pupils, parents, staff, volunteers and governors are made aware of the acceptable use agreement regarding the acceptable use of the school's IT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

8.2. 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 and visitors (where relevant) to ensure they comply with the above. More information is set out in the acceptable use agreements.

9. Pupils using mobile devices in schools

9.1. Please see the Mobile Phone Policy available on the trust website.

10. Staff using work devices outside school

10.1. Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in the trust's Data Protection Policy and Code of Conduct.

10.2. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

10.3. Any USB devices containing data relating to the school must be encrypted. If staff have any concerns over the security of their device, they must seek advice from IT.

11. How schools will respond to issues of misuse

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

11.2. Where a staff member misuses the school's IT 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 which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

12. Training

12.1. 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.

12.2. 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).

12.3. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

13. Filters

13.1. All trust internet connections are subject to internet access controls. These controls restrict the type of internet connections that can be established.

13.2. By default, general web traffic (HTTP and HTTPS) is permitted. Other types of connections will be subject to review. All web traffic is filtered as defined by filter categories in addition to cleared lists and barred lists to supplement the categories where required. The filter categories must be regularly updated and include blacklists as defined by the Internet Watch Foundation.

13.3. Whilst every effort will be made to ensure inappropriate content is not accessible, the trust recognises that some inappropriate access could still be possible. The trust mitigates against the impact of this gap through appropriate education of all users, and additional safety mechanisms, such as computer monitoring software.

14. Artificial Intelligence

14.1. 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 Gemini. The trust 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.

14.2. The trust will treat any use of AI to bully pupils in line with our Behaviour Policy.

14.3. 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.

15. Monitoring Arrangements

15.1. In accordance with our IT usage policy, all connections have their traffic monitored. This not only provides a method of safeguarding, but also helps to maintain the security of our network and provides an audit trail, should one be needed.

15.2. All connections to the internet are monitored, and where possible capturing the username, date, time and URL that is accessed. All schools use robust web filtering and logging to monitor internet usage. DSL and safeguarding teams will be informed of any concerns. All computer workstations also have monitoring software installed, which will:

- Monitor sites accessed on the internet.
- Monitor applications used on the computer.
- Capture keystrokes, alerting appropriate staff to specific keywords that are typed.
- Provide remote monitoring and control of computers for use by teachers and IT services

15.3. All trust computers are protected by a number of different mechanisms to keep the computers and all users safe. These protections will include:

- Specific policies to limit the administrative access of the device.
- Firewalls and anti-virus software to protect against malicious attack of the device.
- Regular software update processes to automatically patch vulnerabilities.

15.4. This Online Safety Policy is linked to our:

- Child Protection and Safeguarding Policy.
- Behaviour Policy.
- Staff Disciplinary Procedures and Code of Conduct.
- Data Protection Policy and Privacy Notices.
- Complaints Procedure.