



BATH & WELLS
Multi Academy Trust

'That they may have life, life in all its fullness' John 10:10

Online Safety policy

Bath and Wells Diocesan Academies Trust

Online Safety Policy

Version number	V2
Last approval date	September 2023
Current date approved	March 2026
Next review date	September 2028
Approved by	SLT
Policy Owner	Director of Operations
Policy Location	SharePoint
Target Audience	All staff, members, pupils and parents/carers
Document History	
Version 1 – Date of Review	January 2026
Version 1 – Revision summary	NA

Context

The Bath & Wells Diocesan Academies Trust (the Trust) is a dynamic learning community committed to providing a safe and supportive environment where pupils and staff can learn, thrive, and flourish. This policy supports that vision by promoting responsible, secure, and ethical use of digital technology across the Trust and its schools. Trust policies are a formal way of documenting the procedures and values of the Trust and are designed to provide an instant picture of the principles of the Trust. They form an important framework that will ensure consistency in applying the agreed values and principles across all elements the Trust.

The Trust recognises that online safety is an integral element of safeguarding and child protection. As technology continues to evolve, pupils encounter new opportunities and risks. This policy ensures that pupils, staff and families understand how to engage with digital platforms in a way that is safe, respectful and aligned with our Christian values.

The Trust Senior Leadership Team determines the review cycle and are responsible for implementation, and monitoring.

Purpose

The purpose of this policy and associated procedures is to outline the Trust's approach to online safety, ensuring that all members of our community can use digital technologies responsibly and securely.

It sets out how online safety is embedded within our curriculum, how staff are supported to uphold good practice, and how we safeguard pupils from risks associated with digital technologies.

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, misinformation, disinformation (including fake news), conspiracy theories, 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 the user 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

The policy and procedures aim to ensure that:

- Pupils and staff understand the importance of online safety and behave responsibly online.
- Clear guidance exists for the acceptable use of technology within Trust schools.
- Effective systems are in place for filtering, monitoring, and responding to misuse.

- Parents and carers are informed partners in promoting online safety.

Scope

This Online Safety Policy applies to all members of the school community (including staff, learners, members, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where [allowed](#)).

Keeping Children Safe in Education 2025 (KCSIE) sets out statutory responsibilities for Trusts. Online safety is now considered part of everyone's safeguarding responsibilities and requires a whole-school approach. The policy and associated procedures cover:

- The teaching of online safety within the Trust curriculum.
- The use of the internet and digital technologies, including mobile devices.
- Expectations for staff use of work devices and online communication.
- Procedures for managing incidents of online misuse and cyber-bullying.

In addition to the responsibilities of KCSIE, the Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying and inappropriate use of social networking by pupils and staff, which may take place out of school, but are linked to membership of the school. It applies to both staff and pupil use of technology for learning.

Trust Alignment

This policy supports the delivery of Health & Safety/Estates priority 3 in our Trust Strategic Plan:

Raise and maintain awareness of the increasing risks and threats to our pupils physically and digitally, ensuring all our schools provide immediate help, support and interventions to keep them safe.

By promoting a culture of safe, ethical and responsible digital engagement, we enable both staff and pupils to flourish in an increasingly digital world.

Other Related Policies

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance - [Keeping Children Safe in Education 2025](#) (KCSIE) and its advice to schools on:

- [Teaching online safety in schools](#) (DfE)
- [Preventing and tackling bullying](#) (DfE)
- [cyber-bullying: advice for headteachers and school staff](#) (DfE)

This policy should be read in conjunction with the following national & Trust policies:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Acceptable Use Policies for Staff, Governors and Volunteers
- Acceptable Use for Pupils & Parents (Trust Template Policies for Schools to edit)
- Data Protection Policies
- Acceptable Use Policies/Agreements
- Data Protection Policies
- ICT Security Policy
- Filtering and Monitoring Standards (DfE, 2024)

Monitoring

This policy is owned by the Director of Operations and will be subject to review by the Senior Leadership Team every three years or sooner if there are changes in technology or guidance. As part of a three yearly review, the Director of Operations will provide a report to the Senior Leadership Team on the impact of the policy via the SWGfL 360 Tool.