BISHOP BEWICK CATHOLIC EDUCATION TRUST

Online Safety Policy

Policy approval record

DOCUMENT CONTROL			
Document title	*BBCET Online Safety Policy*	**Version**	*1*
Document status	*Approved*	**Document type**	*Policy*
Approved by	*Acting Deputy CEO*	**Lead author**	*Acting Deputy CEO*
Applies to	*All school and Trust settings*	**Policy scope**	*Trust-wide*
Related documents	*Safeguarding and Child Protection Policy, Data Protection Policy, Acceptable Use Policy, Cyber Security Policy, Generative AI Policy, Social Media Policy, Data Retention Policy.*		
APPROVAL AND REVIEW			
Approval body	*Trust Board/Executive Team*	**Date approved**	*September 2026*
Effective from	*September 2026*	**Next review date**	*September 2027*
Review cycle	*Annual*		
CHANGE CONTROL			
Summary of changes	*N/A*		
Controlled master location	*BBCET Trust Policy Documents SharePoint*		

BISHOP BEWICK CATHOLIC EDUCATION TRUST

Online Safety Policy

Contents

1. Context 3
2. Purpose 4
3. Roles and Responsibilities 5
4. Reporting and Responding 6
5. Online Safety Education 6
6. Artificial Intelligence (AI) 7
7. Filtering and Monitoring 8
   Filtering 8
   Monitoring 8
8. Technical Security 9
9. Mobile Technologies 10
10. Social Media 11
11. Digital and Video Images 11
    Online Publishing 12
12. Incident Reporting 12
    Responding to Misuse 13
13. Monitoring, Review and Evaluation 13

1. Context

Bishop Bewick Catholic Education Trust (BBCET) recognises that digital technologies are central to teaching, learning, communication and school operations. The Trust is committed to providing a safe digital environment in which children, young people and adults can use technology confidently, responsibly and securely. Online safety is a safeguarding matter and forms part of the Trust's wider culture of child protection.

The DfE Keeping Children Safe in Education statutory guidance requires Local Authorities, Multi Academy Trusts, and schools in England to ensure learners are safe from harm:

"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate."

"Governing bodies and proprietors should ensure online safety is a running and interrelated theme whilst devising and implementing their whole school or college approach to safeguarding and related policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead (and deputies) and any parental engagement."

KCSIE identifies four broad categories of online risk:

"The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

- ***Content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,*
- ***Contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this; for example: 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; for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and*
- ***Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/)."*

2. Purpose

This policy applies to all pupils, employees, governors, volunteers, contractors and visitors across BBCET.

The purpose of this policy is to promote the safe, responsible and effective use of digital technologies and online services across the Trust. It establishes clear expectations for the use of technology, supports the Trust's safeguarding responsibilities and ensures that appropriate systems are in place to identify, manage and respond to online safety concerns.

This policy aims to support staff in protecting children from online harm and ensuring that appropriate measures are in place to identify, manage and respond to concerns relating to online safety. The policy also seeks to protect Trust systems, networks and information assets from misuse, compromise or damage, whilst promoting the safe, ethical and lawful use of technology across school communities.

Through this policy, BBCET aims to promote awareness of online safety across the Trust, provide guidance and support to staff, and ensure that children are equipped with the knowledge, skills and understanding required to navigate the online world safely and responsibly.

This policy should be read alongside the Trust Safeguarding and Child Protection Policy, Acceptable Use Policy, Data Protection Policy, Cyber Security Policy, Generative AI Policy and Social Media Policy.

3. Roles and Responsibilities

The Trust Board has overall responsibility for ensuring that appropriate online safety arrangements are in place across BBCET and for seeking assurance that schools meet their safeguarding and statutory responsibilities.

Headteachers are responsible for implementing this policy within their schools and ensuring that online safety is embedded within safeguarding arrangements, curriculum provision and staff training.

Designated Safeguarding Leads (DSLs) have operational responsibility for online safety and will oversee the management of concerns, incidents and safeguarding responses.

IT support providers and staff are responsible for maintaining secure systems, implementing appropriate filtering and monitoring arrangements, and supporting schools in meeting relevant DfE standards and Trust requirements.

All staff are expected to understand that online safety is part of safeguarding, follow Trust policies and report concerns immediately.

Pupils are expected to use digital technologies safely, responsibly and in accordance with school expectations and acceptable use requirements. Parents and carers play an important role in supporting the safe and responsible use of technology and are encouraged to work in partnership with schools to reinforce online safety messages and promote positive online behaviours.

Governors and Trustees should ensure that appropriate filtering and monitoring arrangements are in place and regularly review their effectiveness. They should work with school leaders, Designated Safeguarding Leads and technical specialists to understand safeguarding risks relating to technology and support continuous improvement of online safety arrangements.

4. Reporting and Responding

All members of the school community are expected to report online safety concerns and incidents through established safeguarding and reporting procedures.

Where a concern relates to the Headteacher, it will be referred to the Chief Executive Officer.

Where a concern presents a safeguarding risk, involves suspected criminal activity or has the potential to cause significant harm, it will be escalated immediately through safeguarding procedures and, where appropriate, referred to external agencies. Such concerns may include, but are not limited to:

- child sexual abuse material (CSAM);
- child sexual exploitation or grooming;
- the sharing of nude or semi-nude images;
- cybercrime offences, including offences under the Computer Misuse Act 1990;
- terrorism, radicalisation or extremism;
- hate crime or discriminatory abuse;
- online harassment, stalking, fraud or extortion; and
- other illegal, harmful or exploitative online activity.

Schools will ensure that appropriate support is available to those affected by online safety incidents.

5. Online Safety Education

Schools should offer a progressive programme of online safety education that is age-appropriate, responsive to emerging risks and aligned with national guidance. Online safety education should be embedded across the curriculum and wider safeguarding provision to support pupils in developing the knowledge, skills and resilience required to navigate the online world safely.

Pupils should be taught how to stay safe online, manage their digital footprint, identify misinformation and disinformation, recognise online exploitation and abuse, understand the risks associated with social media and emerging technologies, and report concerns appropriately. Responsible online behaviour, respect for others, digital citizenship, copyright awareness and the safe and ethical use of artificial intelligence (AI) technologies should be promoted across schools. Online safety education should take account of pupils' age, stage of development and individual needs, including the needs of vulnerable pupils and those with SEND.

Staff should be supported to understand their responsibilities in relation to online safety, digital professionalism, cyber security, information governance and the use of AI. Additional training should be provided where required to individuals with specific safeguarding or leadership responsibilities.

Where appropriate, external agencies, community organisations and specialist providers may be engaged to support online safety education, awareness raising and safeguarding initiatives that enhance provision and promote positive outcomes for pupils and families.

6. Artificial Intelligence (AI)

BBCET recognises the benefits of artificial intelligence (AI) in supporting teaching, learning, administration and wider school operations. The Trust also recognises that AI technologies present risks relating to safeguarding, data protection, bias, misinformation, intellectual property and the accuracy of outputs.

The use of AI must be safe, responsible, ethical and compliant with relevant legislation, including KCSIE and UK GDPR. The safeguarding of pupils and staff will remain paramount in all decisions relating to the use of AI.

Learning about AI should be incorporated into the curriculum where appropriate, enabling pupils to understand its opportunities, limitations, risks and wider ethical implications. Pupils should be supported to engage critically and responsibly with AI technologies and to recognise that AI-generated content may be inaccurate, misleading or biased.

Training and guidance relating to the use of AI should form part of the Trust's wider programme of safeguarding, online safety, cyber security and data protection training. Staff, governors and trustees should be supported to develop an understanding of the opportunities and risks associated with AI technologies relevant to their role.

Staff must ensure that the use of AI complies with the Trust's Data Protection Policy, Generative AI Policy, Acceptable Use Policy and Cyber Security Policy. Personal, confidential, sensitive or business-critical information must not be entered into AI systems.

Human oversight must remain central to the use of AI. AI should support, not replace, professional judgement and decision-making. Responsibility for decisions, communications and published content remains with the individual using the technology. AI-generated content should be reviewed, fact-checked and assessed for accuracy, appropriateness and potential bias before it is relied upon or shared.

Appropriate consideration should be given to copyright, intellectual property rights and the ethical use of content generated through AI technologies. Schools should also consider the potential impact of AI systems on equality, fairness and safeguarding when evaluating and implementing new technologies.

Any concerns relating to the misuse of AI, data breaches, safeguarding risks or inappropriate outputs should be reported and managed in accordance with Trust Safeguarding and Child Protection Policy and Data Protection Policy.

7. Filtering and Monitoring

Appropriate filtering and monitoring arrangements should be implemented across all BBCET schools and services as part of the Trust's wider safeguarding framework. Arrangements should be reviewed at least annually to ensure they remain effective, proportionate and responsive to changes in technology, emerging safeguarding risks and patterns of online safety incidents and behaviours. Filtering and monitoring provision should meet the requirements of *Keeping Children Safe in Education* (KCSIE), relevant statutory guidance and the DfE's Digital and Technology Standards for Schools and Colleges.

The implementation, oversight and review of filtering and monitoring arrangements should involve school leaders, Designated Safeguarding Leads (DSLs), technical specialists and the relevant governor responsible for safeguarding and/or online safety. Responsibility for filtering and monitoring arrangements should be clearly defined and documented at school level.

Where monitoring systems involve the processing of personal data, appropriate data protection arrangements should be completed in accordance with the Trust's Data Protection Policy.

The DfE *Filtering and Monitoring Standards for Schools and Colleges* state:
"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

The DfE defines filtering as:
"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."

Appropriate filtering arrangements should be applied across Trust-managed systems and internet services to help prevent access to illegal, harmful or inappropriate content. Filtering should support safeguarding arrangements and reflect the age and needs of pupils. Filtering provision should support the prevention of access to child sexual abuse material, terrorist and extremist content, and other illegal online material.

Monitoring

The DfE defines monitoring as:
"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."

Monitoring arrangements should support the timely identification of safeguarding concerns and enable appropriate action to be taken where risks are identified. The oversight of monitoring arrangements should involve school leaders, DSLs and technical specialists as appropriate. Concerns identified through monitoring processes should be managed in accordance with safeguarding procedures and recorded in line with school and Trust requirements.

8. Technical Security

Appropriate technical and organisational measures should be maintained across all BBCET schools and services to support safeguarding, protect personal data and ensure the security of Trust systems and information assets.

This includes:

- Technical security arrangements overseen by school leaders, with responsibility delegated to appropriate staff and technical specialists where required.
- Access rights to systems, devices and information being appropriately controlled, reviewed regularly and limited to authorised users.
- All users being responsible for the security of their usernames, passwords and authentication methods and reporting any suspected security breach immediately.
- Password management arrangements being implemented in accordance with Trust information security requirements.
- Trust networks, systems and devices being protected through appropriate technical controls, including secure configuration, endpoint protection, firewalls and access controls.
- Appropriate arrangements being in place to protect systems from unauthorised access, malicious activity and cyber threats.
- Secure and tested backup arrangements being maintained to support business continuity and recovery.
- Software, applications and operating systems being appropriately licensed, supported and regularly updated.
- School-issued devices being managed and used in accordance with Trust policies and acceptable use requirements.
- Personal use of technology on school systems being governed by the Trust's Acceptable Use Policy.
- Staff not installing unauthorised software or applications onto Trust devices.
- Appropriate measures being in place to protect personal and sensitive information, including encryption where required and the secure storage and transfer of data.
- Mobile devices accessing school systems being subject to appropriate security and management controls.
- Guest access to school systems being controlled and proportionate to identified risks.
- Appropriate controls being in place to prevent the unauthorised sharing, disclosure or loss of personal or confidential information.
- Care being taken when using artificial intelligence (AI) technologies to ensure that personal, confidential, sensitive or business-critical information is not entered into systems which have not been approved for that purpose.
- Multi-factor authentication being used where appropriate to protect sensitive information and remote access to school systems.
- AI technologies used within technical security or monitoring arrangements being subject to appropriate oversight, review and assurance to ensure their effectiveness, accuracy and fairness.

Further information relating to information security, cyber security arrangements and technical controls can be found within the Trust's Data Protection Policy, Cyber Security Policy and Generative AI Policy.

9. Mobile Technologies

Schools should ensure that the use of mobile technologies is managed in accordance with the Trust's Safeguarding and Child Protection Policy, Acceptable Use Policy, Data Protection Policy and Cyber Security Policy.
This includes:

- Clear expectations being established regarding the use of school-issued and personal devices by pupils, staff and visitors.
- Appropriate controls being in place to manage access to Trust systems, networks and online services.
- Mobile devices being used in a manner that supports educational purposes and does not compromise safeguarding, learning, wellbeing or professional standards.
- Appropriate filtering and monitoring arrangements being applied where devices access Trust-managed networks and services.
- Personal, confidential or sensitive information being accessed, stored and transferred only in accordance with Trust data protection and information security requirements.
- School-issued devices being subject to appropriate management, security and oversight controls.
- Access to devices and digital resources being managed fairly and appropriately to support learning.
- Appropriate arrangements being in place to manage loss, theft, misuse or damage to devices.
- Pupils receiving education regarding the safe, responsible and respectful use of mobile technologies both within and beyond the school environment.
- Staff maintaining appropriate professional boundaries and not using personal devices or communication channels inappropriately with pupils.
- The taking, storing and sharing of photographs, audio recordings and video content being managed in accordance with safeguarding requirements and Trust procedures.
- Personal devices being used on Trust premises only in accordance with school expectations and acceptable use requirements.
- Any misuse of mobile technologies being managed in accordance with safeguarding procedures, behaviour expectations and relevant Trust policies.

Users are expected to act responsibly and safely when using mobile technologies. Any concerns relating to misuse, inappropriate content, online safety risks or potential safeguarding issues should be reported immediately through established safeguarding and reporting procedures.

Further information relating to mobile device security, acceptable use, data protection and safeguarding requirements can be found within the Trust's Safeguarding and Child Protection Policy, Data Protection Policy and Acceptable Use Policy.

10. Social Media

The use of official school or Trust social media accounts should be undertaken in accordance with the Trust Social Media Policy and any locally agreed procedures.

Staff should maintain appropriate professional standards at all times and must not use personal social media accounts to communicate directly with pupils. Personal use of social media should not compromise professional standards, safeguarding responsibilities, confidentiality requirements or the reputation of the Trust and its schools.

Where a personal account identifies, refers to, or may reasonably be associated with a BBCET school, the Trust or an individual's professional role, it should be made clear that any views expressed are personal and are not made on behalf of the school or the Trust.

The Trust and its schools may monitor publicly accessible online content where there is a legitimate reason to do so, including safeguarding concerns, reputational issues or matters relating to the safety and wellbeing of pupils, staff or the wider school community. Concerns raised through social media should be resolved through established school and Trust procedures. Parents and carers expressing concerns via social media should be encouraged to contact the relevant school directly.

Pupils should be supported in understanding the risks associated with social media and encouraged to use social networking services responsibly, respectfully and safely. Schools should address social media use through online safety education, behaviour expectations and safeguarding arrangements.

11. Digital and Video Images

Schools should ensure that the creation, storage, use and publication of images and video content is undertaken in accordance with the Trust Safeguarding and Child Protection Policy, Data Protection Policy and Social Media Policy.

This includes:

- Pupils being educated about the safe, responsible and respectful creation, use and sharing of images and video content.
- Appropriate consent arrangements being in place for the use and publication of images.
- Staff being aware of pupils whose images must not be taken, stored or published.
- Images and video for school purposes being created, stored and shared using approved systems and devices.
- Photographs, videos and other media being selected carefully and used appropriately to protect the privacy, dignity and safety of those featured.
- Full names not being published alongside images of pupils unless there is a clear and lawful reason to do so.
- Parents and carers being informed about how images will be used, stored and retained.
- Images being stored securely and retained in accordance with the Trust's Data Retention Policy.
- The use of live-streaming and video-conferencing technologies being managed in accordance with safeguarding requirements and relevant national guidance.

Online Publishing

BBCET schools communicate with pupils, parents, carers and the wider community through a range of digital channels, including websites, newsletters, social media and other online platforms.

Schools should ensure that all online publishing is managed appropriately and complies with safeguarding, data protection, copyright and intellectual property requirements. Information published online should be accurate, appropriate and consistent with school values and expectations.
This includes:

- Protecting the identity and personal information of pupils when publishing content online.
- Ensuring that images, videos and pupil work are published appropriately and with any required permissions.
- Complying with copyright, intellectual property and data protection requirements.
- Maintaining professional standards in all online communications.
- Providing appropriate contact details and routes for raising concerns or reporting online safety issues.
- Making relevant policies, guidance and online safety information available through the school website where appropriate.

Online publishing should support engagement with families and communities whilst maintaining the safety, privacy and wellbeing of pupils and staff.

12. Incident Reporting

Online safety incidents and concerns should be managed in accordance with safeguarding procedures and relevant policies.

Where an online safety issue, incident or concern arises:

- concerns should be reported through established safeguarding and reporting procedures;
- concerns relating to pupils should be managed through safeguarding processes led by the Designated Safeguarding Lead (DSL);
- concerns relating to staff should be managed in accordance with safeguarding, disciplinary and allegations procedures;
- appropriate support should be provided to those affected;
- incidents should be recorded, investigated and escalated where required; and
- the response should take account of the needs of those involved and the wider school community.

Schools should ensure that staff receive appropriate training and guidance to respond effectively to online safety concerns including cyberbullying, online abuse, exploitation, inappropriate content, harmful online behaviour and safeguarding risks.

Responding to Misuse

The Trust expects all users of digital technologies to act responsibly and in accordance with this policy and the Trust's Acceptable Use Policy. Inappropriate or unlawful use of technology should be managed proportionately and in accordance with relevant safeguarding, behaviour, disciplinary and legal requirements.

Where misuse is suspected, schools should ensure that:

- concerns are investigated appropriately by authorised staff;
- evidence is preserved where required;
- safeguarding procedures are followed at all times;
- appropriate records are maintained; and
- incidents are escalated to external agencies where necessary.

Where criminal activity or illegal content is suspected, staff should not undertake their own investigation beyond what is necessary to safeguard those involved and preserve evidence. Advice should be sought immediately from the police and other relevant agencies.

Any device, account or system believed to contain evidence of illegal activity should be secured and preserved in accordance with safeguarding and legal requirements.

13. Monitoring, Review and Evaluation

The effectiveness of online safety arrangements should be monitored regularly through safeguarding practice, incident trends, training records and filtering and monitoring reviews.

This policy will be reviewed at least annually, or sooner where required due to changes in DfE legislation, statutory guidance, technology, safeguarding requirements or significant incidents.