Bidborough Church of England Primary School

Faith in Our Future

Online Safety Policy

Approved by	FGB
Date approved	September 2026
Reviewed by	Designated Safeguarding Lead & Deputy Headteacher
Date of next review	Autumn 2027
Policy reference	Kent model/KCSIE 2026

Faith in Our Future

Matthew 13:31-32 – The Kingdom of heaven is like a mustard seed…Though it is the smallest of all seeds, yet when it grows, it is the largest of garden plants and becomes a tree, so that the birds come and perch in its branches.

Our life together at Bidborough Church of England Primary School is rooted in Christ's words describing how a little faith can make all things possible. With the values of love, hope, forgiveness, courage and koinonia underpinning all that we do, we seek to prepare all to step out into the world reflecting God's love for one another. With 'Faith in Our Future' we encourage all to:

- *Grow confidently, as a responsible, life-long learner*
- *Achieve highly, not only in academic areas but in their own personal goals*
- *Contribute successfully, as a member of the wider community*
- *Enjoy life, feeling prepared for every stage of life's journey*

Online Safety Policy

CONTENTS

1. Important Contacts
2. Aims
3. Legislation and Guidance
4. Definitions
5. Roles and Responsibilities
6. Education and Curriculum
7. Filtering and Monitoring
8. Artificial Intelligence
9. Mobile Phones, Cameras and Smart Devices
10. Remote Learning
11. Cyberbullying
12. Child-on-Child Abuse Online
13. Sharing Nudes and Semi-Nudes
14. Online Sexual Violence and Harassment
15. Online Child Exploitation
16. Radicalisation and Extremism
17. Cybercrime
18. Data Security
19. Reporting Concerns
20. Working with Parents and Carers
21. Monitoring Arrangements
22. Links with Other Policies
Appendix 1 Support Services

Online Safety Policy

1. IMPORTANT CONTACTS

See contact table below

Role	Name	Contact Details
School Designated Safeguarding Lead (DSL)	Julie Burton	01892 529333 Headteacher@bidborough.kent.sch.uk DSL@bidborough.kent.sch.uk
School Deputy Safeguarding Leads (Deputy DSL)	Jane Bateup Fiona Gordon Katherine Housley Sarah Lindley Leah Markwell	01892 529333 jbateup@bidborough.kent.sch.uk fgordon@bidborough.kent.sch.uk khousley@bidborough.kent.sch.uk slindley@bidborough.kent.sch.uk lmarkwell@bidborough.kent.sch.uk
Safeguarding Governor	Ian Torpey	Via School Office
Kent Front Door		03000 411111
Police	Emergency	999
Police	Non-Emergency	101
CEOP		www.ceop.police.uk

2. AIMS

At Bidborough Church of England Primary School, we recognise that technology and the internet play a significant role in the lives of children and families. Online technologies provide valuable opportunities for learning, creativity, communication and collaboration, but also present safeguarding risks that must be managed effectively.

The aims of this policy are to:

- Safeguard and promote the welfare of all pupils online.
- Ensure pupils use technology safely, responsibly and respectfully.
- Protect children from online abuse, exploitation, harm and inappropriate content.
- Establish clear procedures for responding to online safety concerns.
- Support staff, governors and parents in promoting online safety.
- Meet statutory safeguarding requirements and the expectations of KCSIE 2026.

Online safety is a safeguarding issue and forms an integral part of the school's wider safeguarding culture. The school is committed to developing pupils as responsible digital citizens who are equipped with the knowledge, skills and resilience needed to navigate the online world safely.

3. LEGISLATION AND GUIDANCE

This policy is based on Keeping Children Safe in Education 2026, Working Together to Safeguard Children 2026, EYFS, UK GDPR, Prevent and UKCIS guidance.

4. DEFINITIONS

Online safety risks are grouped into Content, Contact, Conduct and Commerce risks. 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, 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, 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 using AI and online bullying; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

5. ROLES AND RESPONSIBILITIES

Online safety is everyone's responsibility and forms part of the school's whole-school safeguarding approach.

Governors will: ensure compliance with KCSIE 2026; review online safety arrangements and filtering and monitoring effectiveness annually; ensure appropriate resources and training are available; and provide strategic challenge regarding online safety and safeguarding.

The Headteacher will: oversee implementation of this policy; support the DSL; ensure appropriate filtering and monitoring arrangements; ensure staff receive suitable training; and promote a strong culture of online safety throughout the school.

The DSL will: take lead responsibility for online safety; oversee filtering and monitoring reports; manage online safeguarding concerns; maintain safeguarding records; liaise with external agencies; support staff and parents; and ensure that online safety remains a central safeguarding priority.

All staff will: model safe and responsible technology use; deliver online safety education where appropriate; understand filtering and monitoring processes; follow reporting procedures; and immediately refer concerns to the DSL.

Parents and carers are encouraged to discuss online safety regularly with their children, supervise online activity appropriate to age and maturity, use parental controls where appropriate, and work in partnership with the school when concerns arise.

Pupils are expected to follow Acceptable Use Agreements, behave respectfully online, protect personal information, report concerns promptly, and contribute to a positive and safe online environment.

6. EDUCATION AND CURRICULUM

Online safety is taught progressively through Computing, PSHE, Relationships Education, assemblies and themed activities. Pupils learn about privacy, cyberbullying, online reputation, misinformation, AI and reporting concerns.

7. FILTERING AND MONITORING

The school maintains robust filtering and monitoring systems as part of its whole-school safeguarding arrangements. Filtering and monitoring support the school in protecting pupils from harmful, inappropriate or illegal online content and help identify safeguarding concerns at an early stage.

The Governing Body has strategic responsibility for filtering and monitoring and will review effectiveness at least annually. Governors will ensure that the school meets the DfE Filtering and Monitoring Standards and that appropriate safeguarding measures remain in place.

The Headteacher, DSL and Deputy Headteacher are responsible for overseeing operational arrangements. The Deputy Headteacher leads operational reviews of filtering and monitoring effectiveness and reports findings to the DSL and Governors.

The school will:
- Maintain appropriate filtering on all school devices and networks.
- Ensure monitoring systems are proportionate and support safeguarding.
- Review filtering and monitoring arrangements regularly.
- Record and investigate filtering breaches.
- Escalate safeguarding concerns arising from monitoring activity.
- Ensure staff understand their responsibilities regarding filtering and monitoring.

All staff will receive training on filtering and monitoring expectations as part of safeguarding training and induction. Pupils and parents will be informed that the use of school devices, accounts and networks may be monitored for safeguarding, security and policy compliance purposes.

The school recognises that filtering and monitoring form only one element of safeguarding and do not replace effective education, supervision, behaviour management and professional curiosity.

The school's designated Filtering and Monitoring Lead is the Headteacher. A written record of filtering and monitoring reviews, testing and effectiveness checks will be maintained and reported to Governors annually.

8. ARTIFICIAL INTELLIGENCE (AI)

Generative Artificial Intelligence (AI) tools are now widely available and may include platforms such as ChatGPT, Microsoft Copilot and Google Gemini. The school recognises that AI can support learning, creativity and administrative efficiency; however, it can also present significant safeguarding, ethical and data protection risks.

Potential safeguarding concerns include:
- Exposure to inaccurate, misleading or biased information.
- AI-enabled cyberbullying, harassment and abuse.
- AI-facilitated grooming, coercion and exploitation.
- Creation of deepfakes, manipulated media and synthetic content designed to deceive.

- AI-generated nude or semi-nude imagery, including so-called deep nudes.
- Excessive reliance on AI chatbots for emotional support or companionship.
- Privacy, confidentiality and data protection breaches.

The school will educate pupils about the safe, responsible and critical use of AI technologies through the curriculum and online safety education programme. Pupils will be taught that AI-generated content may not be accurate, trustworthy or appropriate and should be checked against reliable sources.

Staff must follow the school AI Policy at all times and must not enter confidential, safeguarding or personal data into unauthorised AI systems. Any misuse of AI which may place a child at risk will be treated as a safeguarding concern and managed in line with the Child Protection and Safeguarding Policy.

Where concerns involve AI-generated sexual imagery, deepfakes or manipulated images involving pupils, the school will follow UKCIS guidance on sharing nudes and semi-nudes and will refer to external agencies where appropriate.

9. MOBILE PHONES, CAMERAS AND SMART DEVICES

The school recognises that mobile phones, cameras, tablets, wearable technology and other smart devices can support communication and learning but may also present safeguarding risks. Clear expectations are therefore in place for staff, pupils, volunteers, visitors and contractors.

Staff may bring personal devices onto site for their own use; however, use must be limited to non-contact time and must not interfere with professional responsibilities. Staff must not use personal devices to photograph, film or record pupils. Images of pupils may only be taken using school-approved devices and for authorised educational, safeguarding or promotional purposes in accordance with parental permissions and data protection requirements.

In accordance with EYFS safeguarding requirements, personal mobile phones, smart watches and any device capable of recording images, video or audio must not be used in areas where Early Years children are present, except in exceptional circumstances authorised by the Headteacher or DSL. Photographs and videos of children may only be taken using school-approved devices. All images must be stored securely and managed in accordance with the school's data protection procedures.

Visitors, volunteers and contractors must comply with school safeguarding requirements at all times. Personal photography, filming or recording involving pupils is not permitted unless specifically authorised by the Headteacher or DSL.

The unauthorised use of mobile phones, cameras, wearable technology or social media to capture, store, access or share images, recordings or information relating to pupils is strictly prohibited and may result in disciplinary action and/or referral to external agencies where appropriate.

The school operates as a mobile phone free environment for pupils unless specific arrangements have been agreed. Any personal devices brought onto site by pupils must be handed in and stored in accordance with school procedures.

10. REMOTE LEARNING

Approved platforms only will be used. Safeguarding expectations remain unchanged during remote learning.

11. CYBERBULLYING

Cyberbullying is a form of child-on-child abuse and will not be tolerated. Cyberbullying may occur through social media, messaging applications, gaming platforms, email, image sharing or other online technologies. Incidents may take place both inside and outside school and can have a significant impact on a child's wellbeing, safety and attendance.

Examples may include abusive messages, intimidation, exclusion, humiliation, sharing of images without consent, impersonation, threats, prejudice-based bullying and the use of AI-generated content to target others.

All reports of cyberbullying will be taken seriously and investigated promptly. The school will provide support for victims, work with parents and carers, apply appropriate sanctions where necessary and involve external agencies where appropriate. Incidents will be recorded and monitored to identify patterns, trends and safeguarding concerns.

Pupils are encouraged to report concerns immediately and are reminded that they will be supported when doing so. Education regarding respectful online behaviour, digital citizenship and reporting concerns forms part of the school curriculum.

12. CHILD-ON-CHILD ABUSE ONLINE

The school recognises that children can abuse other children online. Online child-on-child abuse can occur between individuals or groups and may take place through social media, messaging applications, gaming environments, shared platforms or other forms of digital communication.

Online child-on-child abuse may include cyberbullying, harassment, coercive behaviour, prejudice-based abuse, exploitation, online sexual harassment, image-based abuse, sharing of nude or semi-nude images, online humiliation and the misuse of AI-generated content.

The school will never dismiss abusive behaviour as banter, a joke, part of growing up or harmless peer conflict. All concerns will be treated seriously and managed through safeguarding procedures.

Where a report is made, the DSL will assess risk, consider the needs of the victim and alleged perpetrator, determine what support is required and decide whether external agencies should be involved. Appropriate safeguarding measures, supervision arrangements and support plans will be implemented where necessary.

The school will actively promote a culture of respect, kindness and safety and will educate pupils about healthy relationships, consent, online behaviour and reporting concerns.

13. SHARING NUDES AND SEMI-NUDES

The sharing of nude or semi-nude images by children is a safeguarding issue and requires an appropriate safeguarding response. This includes photographs, videos, live streams, digitally manipulated images, AI-generated images, deepfakes and so-called deep nudes. The school will follow the latest UK Council for Internet Safety (UKCIS) guidance and local safeguarding procedures.

All incidents involving the consensual or non-consensual sharing of nude or semi-nude imagery must be reported immediately to the DSL. Staff must not view, copy, print, share, save or delete imagery, nor ask a pupil to display or remove content. Staff must reassure pupils, explain that the concern will be passed to the DSL, and record information in accordance with safeguarding procedures.

Following a report, the DSL will undertake an initial risk assessment and determine whether there is an immediate safeguarding risk, whether external agencies should be involved, whether parents should be informed, and what support is required for those involved. Referrals to Children's Services and/or the Police will be made where there are concerns regarding exploitation, coercion, grooming, significant harm, sexual offences, or where an adult is involved.

The school will provide appropriate support for victims, alleged perpetrators and any other pupils affected by an incident. Decisions, actions and outcomes will be recorded securely. Education regarding image sharing, consent, online pressure, legal consequences and reporting concerns will be delivered through Relationships Education, PSHE and online safety education.

Where AI-generated or digitally manipulated imagery is involved, the school will respond in the same way as for any other incident involving nude or semi-nude imagery and will consider any additional safeguarding risks arising from deepfake technology or image manipulation.

14. ONLINE SEXUAL VIOLENCE AND HARASSMENT

The school recognises that sexual violence and sexual harassment can occur both online and offline and that online incidents may be part of a wider pattern of abuse. Such behaviour is never acceptable and will never be dismissed as banter, part of growing up, or harmless behaviour. All reports will be taken seriously and responded to promptly.

Online sexual violence and sexual harassment may include unwanted sexual comments, sexualised bullying, requests for sexual images, sharing of explicit content, sexual intimidation, coercive behaviour, image-based abuse, up-skirting, abusive use of social media, and AI-generated sexual content or manipulated imagery.

All victims will be reassured that they are being taken seriously and will be supported and kept safe. The school will ensure that no victim is made to feel responsible for the abuse they have experienced.

On receiving a report, the DSL will undertake an immediate risk assessment. The assessment will consider the needs and wishes of the victim, the risks posed by the alleged perpetrator, the impact on other pupils, and whether external agencies need to be involved. The assessment will be recorded and reviewed regularly.

Where appropriate, referrals will be made to Children's Services, the Police and other specialist agencies. The school will work closely with parents and carers unless doing so would place a child at additional risk of harm.

Support may include pastoral support, safety planning, timetable adjustments, supervision arrangements, counselling, and referrals to external services. Sanctions may be applied where appropriate in line with the Behaviour Policy and safeguarding procedures.

The school will also use information from reports to review policies, procedures, staff training and curriculum provision to help prevent future incidents and promote a culture of respect and safety.

15. ONLINE CHILD EXPLOITATION

The school recognises that children may be vulnerable to online child sexual exploitation (CSE) and child criminal exploitation (CCE). Online exploitation can occur through social media, gaming platforms, messaging services, livestreaming platforms and other online environments. Children may be groomed, manipulated, coerced, blackmailed or encouraged to engage in behaviours which place them at risk.

Indicators may include secrecy around online activity, receipt of gifts, unexplained relationships, inappropriate sexualised behaviour, significant changes in behaviour, involvement in criminal activity or repeated exposure to unsafe online situations.

All concerns will be reported immediately to the DSL. The DSL will undertake a risk assessment, liaise with parents where appropriate, and make referrals to Children's Services, Police, CEOP or other agencies as required. The school will provide support and protective measures for affected pupils and will ensure concerns are recorded securely.

16. RADICALISATION AND EXTREMISM

The school fulfils its responsibilities under the Prevent Duty and recognises that pupils may be vulnerable to extremist influences online. Extremist content may be encountered through websites, social media platforms, forums, messaging applications, livestreams, gaming environments and AI-enabled systems. Staff will remain vigilant for indicators of radicalisation and will report concerns immediately to the DSL. The DSL will assess concerns, seek advice where necessary and make referrals to appropriate agencies, including Channel, where appropriate.

The curriculum promotes critical thinking, respect, tolerance, democracy, the rule of law and individual liberty. Pupils are taught to challenge misinformation, manipulation and harmful ideological content encountered online.

17. CYBERCRIME

The school recognises that some children may have an interest in computing, programming, technology and cyber security. While these interests are often positive and should be encouraged, there is a risk that some young people may inadvertently or deliberately become involved in cyber-enabled or cyber-dependent criminal activity.

Cyber-enabled crimes are traditional offences that can be committed online, such as fraud, harassment, blackmail or the distribution of harmful content.

Cyber-dependent crimes are offences that can only be committed through the use of computers, networks or internet-enabled technologies. Examples may include unauthorised access to computer systems, hacking, malware distribution, denial-of-service attacks, password theft, data breaches and unauthorised modification of computer material.

Staff will remain alert to indicators that a child may be involved in cybercrime, including unusual interest in bypassing security systems, attempts to access restricted areas of networks, discussion of hacking activity, use of anonymous accounts or possession of software associated with cyber intrusion.
Any concerns regarding cybercrime will be reported immediately to the DSL. The DSL will assess risk, consider wider safeguarding concerns, liaise with parents and carers where appropriate and seek advice from external agencies. Referrals to the Police or specialist agencies will be made where necessary.

Where appropriate, the school will seek opportunities to channel pupils' interests positively through education, enrichment activities and cyber security programmes. Pupils will be taught about the law relating to cybercrime, ethical use of technology and the consequences of illegal online activity.

18. DATA SECURITY AND INFORMATION MANAGEMENT

The school takes appropriate technical and organisational measures to safeguard personal data, devices, systems and networks. Effective information management and cyber security are essential components of safeguarding and online safety.

The school will:

- Maintain secure passwords and appropriate access controls for staff and pupils.
- Use filtering and monitoring systems to support safeguarding and network security.
- Maintain antivirus, malware protection and security updates on school devices.
- Ensure personal data is stored, processed and transferred securely.
- Restrict access to sensitive information to authorised users only.
- Review cyber security arrangements regularly and respond promptly to emerging risks.
- Ensure data protection requirements are reflected in staff training and induction.

All staff are responsible for protecting information and must comply with the Data Protection Act 2018, UK GDPR, the school Data Protection Policy and all relevant information security procedures. Staff must not share passwords, leave devices unsecured, or store confidential information on unauthorised devices or systems.

Any suspected data breach, cyber security incident, loss of personal data, unauthorised access, phishing attack or compromise of school systems must be reported immediately to the Headteacher, Designated Safeguarding Lead and Data Protection Officer. Incidents will be assessed, recorded and managed in accordance with legal requirements and school procedures.

The school recognises that good information security practice helps protect pupils, staff and families from harm and supports the wider safeguarding culture of the school.

19. REPORTING CONCERNS

All concerns must be reported immediately to the DSL or Deputy DSL.

20. WORKING WITH PARENTS AND CARERS

The school shares information, guidance and support to help parents keep children safe online.

21. MONITORING ARRANGEMENTS

This policy will be reviewed annually by the Governing Body.

22. LINKS WITH OTHER POLICIES

Child Protection and Safeguarding, Behaviour, AI, Data Protection, Acceptable Use, Anti-Bullying and Relationships Education policies.

APPENDIX 1: SUPPORT SERVICES

CEOP – www.ceop.police.uk
Childline – www.childline.org.uk
NSPCC – www.nspcc.org.uk
UK Safer Internet Centre – www.saferinternet.org.uk
Internet Matters – www.internetmatters.org
Internet Watch Foundation – www.iwf.org.uk
Report Harmful Content – www.reportharmfulcontent.com
National Cyber Security Centre – www.ncsc.gov.uk
Childnet – www.childnet.com
KSCMP resources – www.kscmp.org.uk
Professional Online Safety Helpline – www.saferinternet.org.uk/helpline