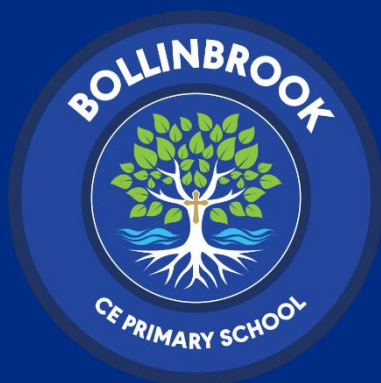




ONLINE SAFETY POLICY

'...like a tree firmly planted by streams of water which yields its fruit...'

Psalm 1v3

Bollinbrook CE Primary School Online Safety Policy

Recommended by	Pupil Welfare
Approved by	Governing Board
Approval Date	September 2026
Version Number	1
Review Date	September 2027
Legal Status	

CHANGE RECORD FORM

Version	Date of change	Date of release	Changed by	Reason for change
2	May 2020	May 2020	L.Le Marinel	Covid-19 update
3	September 2021	September 2021	L.Le Marinel	Policy Review
4	September 2022	September 2022	L.Le Marinel	Policy Review
5	September 2023	September 2023	L.Le Marinel	Policy Review
6	September 2024	September 2024	L.Le Marinel	Policy Review
7	September 2025	September 2025	L.Le Marinel	Policy Review
8	September 2026	September 2026	L.Le Marinel	Policy Review

Mission Statement

...‘a tree firmly planted by streams of water which yields its fruit...’ Psalm 1v3

At Bollinbrook CE Primary the Christian value of ‘Love’ is at the heart of who we are as a community. We teach our children to be rooted in Jesus Christ so they develop a love of learning that supports their academic, emotional and spiritual growth. If rooted in Christ, children can grow into who they were created to be. Based on Psalm 1v3, ‘like a tree firmly planted by streams of water which yields its fruit...’ We are helping our children grow spiritually, emotionally and academically laying firm roots that will provide strong foundations and bear fruit that will help them on the next stage of their educational journey.

This policy includes an appendix which details our safeguarding arrangements for online safety during any further remote learning and school closure.

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, 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
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Promote a culture of safe, respectful and responsible online behaviour across the whole school community.
- Ensure children are protected from emerging online risks including artificial intelligence (AI) generated content, deepfakes, misinformation, online exploitation, cyberbullying and harmful online behaviours.
- Support parents and carers in developing safe online habits and digital resilience at home.

Legislation and guidance

This policy reflects the latest version of Keeping Children Safe in Education and recognises that online safety is a safeguarding issue. It incorporates current guidance relating to:

- Child-on-child abuse online.
- Harmful sexual behaviour.
- Violence against women and girls (VAWG).
- Misogyny and discriminatory behaviour.
- AI-generated content and manipulated imagery.
- Filtering and monitoring standards.
- Online exploitation and coercion.

Online safety is considered through a whole-school safeguarding approach and is embedded within the school's child protection arrangements.

Other relevant guidance:

[Teaching online safety in schools](#) and its advice for schools on [Preventing and tackling bullying and advice for parents/carers on cyber bullying](#) and [searching, screening and confiscation](#) and [sharing nudes and semi nudes, advice for education settings](#)

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 2002](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger 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

The policy also takes into account the [National Curriculum computing programmes of study](#).

Roles and responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is **Mrs Sarah McCubbin** – Designated Safeguarding Governor.

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 ICT systems and the internet (appendix 2)

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and deputy lead are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

- 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 issues or incidents
- Ensuring that any online safety incidents are logged on CPOMs using the information in appendix 5 and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 3 contains a self-audit for staff on online safety training needs)

- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the governing board
- Monitor emerging online safeguarding risks and ensure school procedures remain effective.
- Work alongside the ICT provider to review filtering and monitoring arrangements annually.
- Monitor trends in online safety incidents and report these to governors.
- Ensure online safety concerns involving AI-generated content, manipulated images, online harassment or exploitation are addressed through safeguarding procedures.
- Support parents with information and guidance regarding online safety concerns affecting pupils beyond the school day where these impact on safeguarding or pupil wellbeing.

This list is not intended to be exhaustive.

The ICT manager (Seven11)

The ICT manager is responsible for:

- Putting in place 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 school, including terrorist and extremist material
- Ensuring that the school's ICT systems 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 ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

Filtering and Monitoring

Bollinbrook Primary School recognises its responsibility to maintain effective filtering and monitoring systems in line with Department for Education standards.

The school:

- Identifies clear responsibilities for filtering and monitoring.
- Reviews filtering and monitoring provision annually.
- Conducts regular safeguarding reviews of monitoring reports.
- Ensures appropriate action is taken when concerning online activity is identified.
- Monitors risks across all internet-connected devices used by pupils and staff.

The Headteacher, DSL and ICT provider work together to ensure systems remain effective and proportionate whilst supporting teaching and learning. The Governing Board receives regular assurance that these arrangements remain fit for purpose.

All staff (including wrap around care staff and any volunteers)

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

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) 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 behaviour policy

This list is not intended to be exhaustive.

Parents / Carers

Parents / Carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet and signed electronically via Arbor (appendix 1)

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

What are the issues?, UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>

Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>

Parent factsheet, Childnet International: [Childnet parent fact sheet](#)

Visitors and members of the community

Visitors and members of the community who use the school's ICT 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 (appendix 2).

Educating pupils about online safety

All staff working in school have completed safeguarding training around the 4 Cs (Keeping Children Safe in Education)

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

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism, AI-generated harmful content, deepfakes and manipulated images.

Contact: being subjected to harmful online interaction with other users; 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. Exploitation through online gaming platforms, social media and AI-assisted communication tools.

Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example, 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; Creating, sharing or distributing manipulated images, deepfakes or AI-generated content intended to cause harm or distress.

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. (If a school feels their pupils, students or staff are at risk, they have a duty to report it to the Anti-Phishing Working Group)

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

Artificial Intelligence and Emerging Technologies

The school recognises that artificial intelligence (AI) technologies are increasingly accessible to children and adults.

Pupils will be taught to use AI safely, responsibly and critically.

Education will include:

- Understanding that AI-generated information may be inaccurate.
- Identifying misinformation and disinformation.
- Recognising manipulated images and deepfakes.
- Protecting personal information when using AI tools.
- Understanding copyright, plagiarism and academic honesty.

Any safeguarding concerns relating to AI-generated content, deepfakes, manipulated imagery, impersonation or exploitation will be managed in line with the school's Child Protection and Safeguarding Policy

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.

Online safety will also be covered during parents' evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher who is also the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Parents and carers play a vital role in supporting online safety.

Parents are encouraged to:

- Monitor children's online activity.
- Use age-appropriate parental controls.
- Discuss online risks regularly with their children.
- Report concerns directly to the school.

The school expects all members of the community to communicate concerns respectfully and through appropriate channels. Concerns regarding children, staff or school matters should not be discussed on social media platforms or community forums where confidentiality and safeguarding may be compromised.

Where online behaviour by parents or carers affects the safety, wellbeing or reputation of pupils, staff or the wider school community, the school may take appropriate action in accordance with relevant policies.

Cyber-bullying

Definition

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. (See also the school behaviour policy.)

Online incidents that involve discrimination, misogyny, hate-based behaviour, sharing of intimate images, coercive behaviour or online sexual harassment will be treated as safeguarding concerns and managed through safeguarding procedures as well as behaviour procedures.

Preventing 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. Staff will discuss cyber-bullying with their class and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents 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 school behaviour policy. 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.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the 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 school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

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, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

Pupils using mobile devices in school

Pupils in years 5 and 6 only may bring mobile devices into school providing they have signed the mobile phone agreement now on Arbor (appendix 5), but are not permitted to use them during:

- Lessons
- Before and after school when on site
- Clubs before or after school, or any other activities organised by the school

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside school

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 appendix 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. Staff have secure remote access now and are therefore asked to longer use USB drives for confidential information.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager. Work devices must be used solely for work activities.

Staff must comply with the school's Social Media Policy and maintain appropriate professional boundaries at all times.

Staff must not:

- Accept current pupils as social media contacts.
- Communicate with pupils through personal social media accounts or personal messaging services.
- Share pupil information, photographs or videos through personal devices or accounts.
- Discuss school matters in local community forums or social media groups.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT 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.

Where a staff member misuses the school's ICT 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.

Training

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.

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).

The DSL and deputies will undertake safeguarding training in accordance with current statutory guidance and will update their knowledge regularly, including developments in online safety, filtering and monitoring, online exploitation, AI-related risks and emerging technologies.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

Remote Learning and Virtual Education

Should remote education be required, online safety expectations within this policy, the Child Protection Policy and Staff Code of Conduct will continue to apply. All online communication between staff and pupils will take place through approved school platforms and be subject to appropriate safeguarding procedures.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMs. An incident report log can be found in appendix 4 and this information needs to be recorded electronically under the category of 'Online Safety'.

This policy will be reviewed annually by the Headteacher. At every review, the policy will be shared with the governing board.

Links with other policies

This online safety policy is linked to our:

Safeguarding policy

Behaviour policy

Staff disciplinary procedures

Data protection policy and privacy notices

Complaint's procedure

Social Media Policy

APPENDIX 1: ACCEPTABLE USE AGREEMENT (TO BE SIGNED ON ARBOR)

We at Bollinbrook are mindful of the problems there are with pupils gaining access to undesirable materials on the internet so we have taken steps to deal with this.

We use Smooth wall service which contains a 'firewall' and blocks sites unsuitable for children. This will minimise the chances of pupils encountering undesirable material. If unsuitable websites are located, the page or domain will be blocked. All our screens are in public view at school and normally an adult is present to supervise.

No system is perfect, however, and you should be aware that it is not possible to remove entirely the risk of finding unsuitable material. To this end we need to inform you of the rules which the children are expected to follow to help with our precautions. I would ask you to look through these rules and discuss them with your child and then sign the form in the school registration document.

Bollinbrook School Pupil Internet Agreement

This is to be read through with your parent(s) / guardian(s) and then parents / carers to confirm the agreement on Arbor which is our management system.

At Bollinbrook, we expect all pupils to be responsible for their own behaviour on the Internet, just as they are anywhere else in the school. This includes materials they choose to access, and language they use.

- Pupils using the www are expected not to deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they should report it immediately to a teacher.
- Pupils are expected not to use any rude language in their e-mail communications and contact only people they know or those the teacher has approved. It is forbidden to be involved in sending chain letters.
- Pupils must ask permission before accessing the Internet.
- Pupils should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.
- Homework completed on USB pens may be brought in but it will have to be virus scanned by the teacher before use.
- Personal printing is not allowed on our network, e.g., pictures of pop groups / cartoon characters.
- No personal information such as phone numbers and addresses should be given out and no arrangements to meet someone made unless this is part of an approved school project.
- Pupils consistently choosing not to comply with these expectations will be warned, and subsequently, may be denied access to Internet resources.

APPENDIX 2: ACCEPTABLE USE AGREEMENT (STAFF, GOVERNORS, VOLUNTEERS AND VISITORS)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software
- Share my password with others or log in to the school's network using someone else's details

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):

Date:

APPENDIX 3: ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF

Online safety training needs audit	
Name of staff member/volunteer:	Date:
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

APPENDIX 4: ONLINE SAFETY INCIDENT REPORT LOG (TO BE RECORDED ELECTRONICALLY ON CPOMS)

Online safety incident report log				
Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 5

Mobile Phone Agreement

Years 5 and 6

No children are permitted to bring in mobile phones to school except when requested by the parents of a Y5/6 child who may be making their own way to and from school.

All children must adhere to this agreement if permission has been given to bring in their phones.

- * The phone must be handed in to the office before school or put in the box in the classroom when they enter. All phones will be kept in the office safe.
- * The phones will be taken back to class at the end of the school day by a member of staff.
- * If your child is attending an after-school club, the phone will be kept in the office safe and handed to the child by a member of staff when they leave.
- * The phone must clearly be labelled with the child's name or be clearly identifiable by the child with (for example by the phone case).
- * The phone must not be used on school premises, including outdoor areas.
- * Any mobile phone brought into the school without permission will be confiscated and handed back to the child's parent/carer.
- * The school accepts no responsibility for any loss, damage or theft of the phone if the above steps are not followed by the children and phones are left in bags.

Where mobile phones are used in or out of school to bully or intimidate others, then parents/carers will be invited into school to discuss use of the mobile phone.

Permission to be given via Arbor