Online Safety Policy

St Bartholomew's CE Primary School

Version:	V1.0
Prepared by:	LB
Valid from date:	Autumn term 2024
Valid to date:	Autumn term 2025

Policy Updates	
Version Number	**Changes**
1.0	New Policy

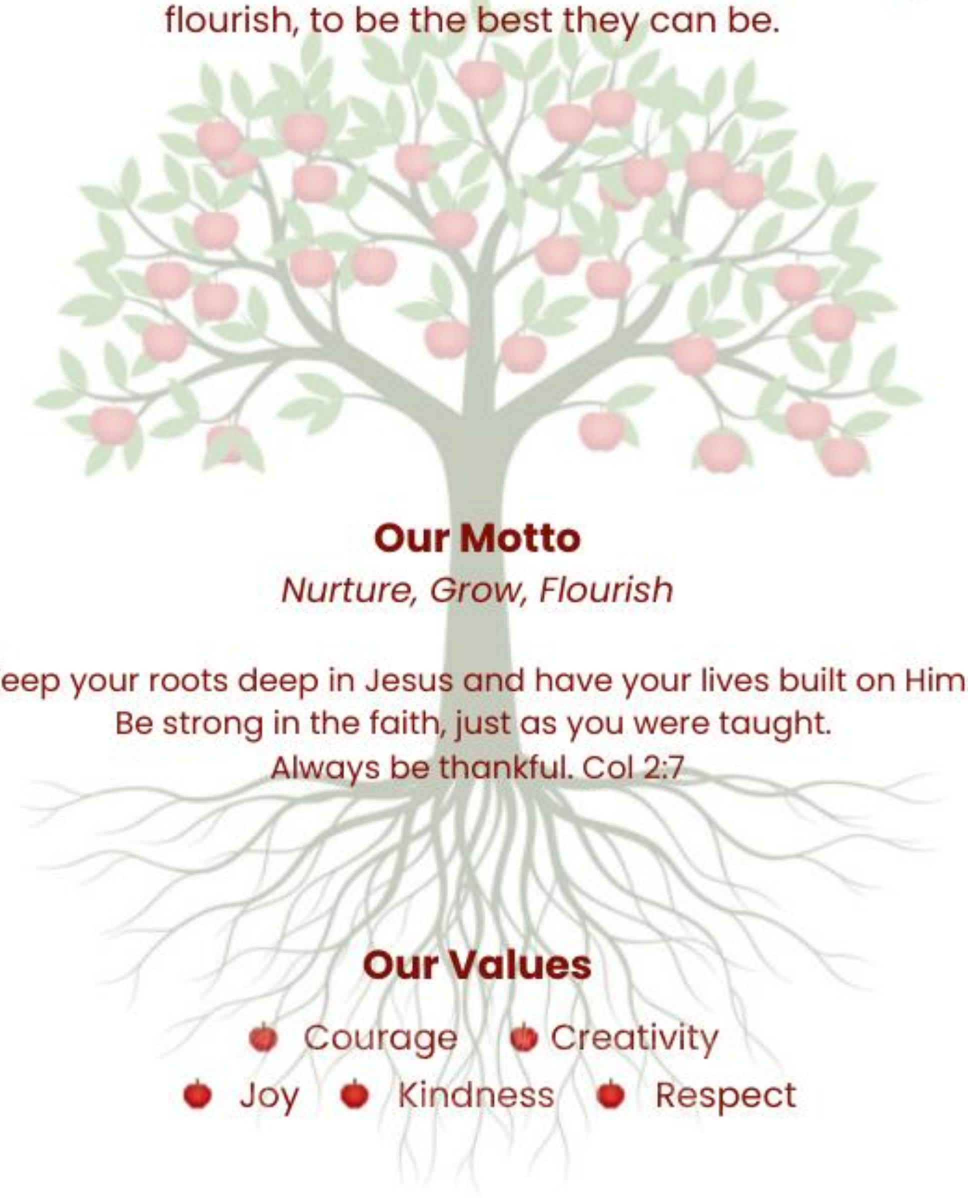
IMPLEMENTATION DATE: December 2024

Contents

Our Vision, Motto and Values

St Bartholomew's Vision

To be a loving and nurturing Christian school community, providing the rich soil that enables our children to develop deep roots, grow and flourish, to be the best they can be.



Our Motto

Nurture, Grow, Flourish

Keep your roots deep in Jesus and have your lives built on Him.
Be strong in the faith, just as you were taught.
Always be thankful. Col 2:7

Our Values

- Courage
- Creativity
- Joy
- Kindness
- Respect

Aims

St Bartholomew's aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, trainee teachers, 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.

Legislation and Guidance

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

The policy also takes into account the National Curriculum computing programs of study.

Roles and Responsibilities

The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the School Leadership Team to account for its implementation.

The Governing Body will hold to account appropriate staff with online safety and monitor online safety information as provided by the school's leadership team.

The Governor who oversees online safety is Beth Riley.

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 IT systems and the internet (appendix 2);

The School Leader

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

The Designated Safeguarding Lead (DSL)

Details of the school's Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Lead (DDSL) are set out in the school's Safeguarding Policy 2024 and are known in each school.

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

- Supporting the School Lead ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with leaders, Computing Co-ordinators, Systems Technician and other internal or external staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged (see appendix 4) 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's 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 such as broadband providers;

This list is not intended to be exhaustive.

The Systems Technician

The systems technician 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 content online while at school, including radicalisation material;
- Ensuring that the school's IT 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 IT systems on a monthly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy;
- Report any incidents of cyber-bullying to School Leaders.

This list is not intended to be exhaustive

All staff

(including supply teachers, Associate/Trainee Teachers, placement students and volunteers)

All staff, including contractors, agency staff, Associate/Trainee teachers, placement students, 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 IT 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 4) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the Behaviour Policy.

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the School Leader 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 IT systems and internet (appendix 1);

Parents/carers 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: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

Information also exists on the school website.

Visitors and members of the community

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

Educating Pupils About Online Safety

All pupils will be taught about E-safety, including online safety, see Computing and PSHE curriculum.

The safe use of social media (including age restrictions) and the internet will also be covered in other subjects where relevant.
Each school will use assemblies/worship to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

Educating parents/carers about online safety

The school will raise parents' awareness of internet safety in letters or other communications and via our website, letters, emails, leaflets or parental workshops. This policy will also be available to parents/carers via our website.

When necessary, online safety will also be covered during parents' evenings or workshops.
If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the class teacher then School Leader or the DSL.

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

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 St. Bartholomew's C.E. Primary School's Behaviour, Safeguarding and Child-on-Child Abuse Policies).

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 aim to educate children so that they know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

We 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 children, 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 may include personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, members of the Governors, Associate/Trainee teachers, placement students 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 sends information/leaflets on cyber-bullying and e-safety 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 – see Appendix 5. Schools may also offer parent workshops when and where appropriate.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the 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 managed appropriately.

The School Leader or DSL/DDSL will report incidents 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/ work against the school culture and ethos.

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 Complaints Policy.

Acceptable Use of The School Internet

All pupils, parents/carers, staff, Associate/Trainee teachers, placement students, volunteers and Governing Body members are expected to sign an agreement regarding the acceptable use of the school's IT 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 monitor the websites visited by pupils, staff, volunteers, Governing Body members and visitors (where relevant) to ensure that they comply with the above. This is done via our monitoring system Securus (up to April 2025); Senso (from April 2025)

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

Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during:

- Lessons
- Activities organised by the school
- For security reasons, all devices must be handed into the school office.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the Behaviour Policy, which may result in the temporary 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, or breach the school's Code of Conduct.

Staff must ensure that their work device is secure and password/code 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. Any USB devices containing data relating to the school must be at least encrypted or ideally not used, as it is the school's preference for data to be stored in its secure online platform.

If staff have any concerns over the security of their device, they must seek advice from the Systems Technician.

Staff should not access and must not store children's information and data on their own devices.

How the school will respond the issues of misuse
Where a pupil 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.

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/ Code of Conduct. 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 – Prevent.

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 deputy/deputies) will undertake child protection and safeguarding training, which ought to include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, ideally at least annually.

Governing Body members 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 Safeguarding Policy.

Monitoring Arrangements
The DSL logs behaviour and safeguarding issues related to online safety on CPOMS. An additional incident report log can be found in appendix 4.

Links with other policies and documents

This online safety policy is linked to:

- Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary Procedures
- Code of Conduct;
- Governor Code of Conduct;
- Data protection policy and privacy notices;
- Complaints procedure;
- Removal of equipment from premises agreement
- Child-on-Child Abuse Policy

Appendix 1: acceptable use agreement (pupils and parents/carers)

Pupil's IT Acceptable User Policy

The school has computers and other devices that enable internet access and facilitate our learning.

These rules will keep everyone safe and help us to be fair to others:

- I will only login as myself.
- I will only open and view my files, or files I have permission to use.
- I will not copy other people's work or anything that is protected by copyright.
- I will use the school IT equipment for school work and homework only.
- I will not download from an external storage device, such as memory stick/drive, or the internet without permission.
- I will ask permission before I use the internet
- When using school IT equipment, I will only communicate with people whom a member of staff has approved.
- The 'communication' I send will be polite, responsible, kind and appropriate.
- I will not give anyone my address, phone number, or any other personal information.
- I will report any unpleasant materials or communication sent to me. I know that my report would be to help protect myself and others.
- I understand my school 'online activity' is being monitored.

Pupils - please sign below to confirm you have read, understand and agree to these rules

Parents/carers – please sign below to confirm that you understand why the school has these rules, that you have discussed them with your child and agree to them.

Parent/Carer: ______________________________

Pupil: ______________________________

Date: ______________________________

Appendix 2: acceptable use agreement (Staff etc)

(Staff, Governors, Associate/Trainee teachers, placement students, volunteers and visitors)

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

Name of staff member/ Trust Board members /Associate/Trainee teacher/ placement student/ volunteer/visitor:

When using the school's IT 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, or that which can influence others into hate or terrorism;
- Use them in any way which could harm the school's or staff member's reputation;
- Use any improper language when communicating with external organisations 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 (unless granted by work colleagues);
- Allow non-staff members to use school or Trust resources.

I will only use the school's IT 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 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 Systems Technician 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 intend to use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed **(staff member/ Trust Board members/Associate/ Trainee teacher/ placement student /volunteer/visitor):**	**Date:**

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/Associate/Trainee teacher/ placement student/ volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school? Who is this?	
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/carers?	
Do you regularly change your password for accessing the school's IT 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

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

Appendix 5: Sample E-safety letter

Dear parents and carers,

Keeping Your Child Safe Online

As we prepare for Christmas, we know that Santa sometimes brings, to children who are very lucky, lots of wonderful electrical Christmas gifts such as: Nintendo Switch, X-Box series X and S, PlayStation 5, iPads, mobile telephones, tablets, laptops and much more. Obviously, these pieces of amazing technology are fun and can also be used for education purposes - for example, TT Rockstars and accessing MS Teams.

We are sure that you agree, that once 'online' with their own device, it is essential your child is safe. Therefore, we wanted to share some e- safety advice. Please monitor carefully what your child is accessing. The recommend user age for TikTok, Snapchat, Instagram and Facebook are 13. Children under the age of 13 should not have a YouTube account. These age restrictions are to protect young children from potentially viewing, inappropriate content. Over the past five years as a national, our mobile data usage has increased ten times. Therefore, it is more likely children access online content via their mobile telephones. The risk with this access is there are less and sometimes no restrictions and filters, as with home and school broadband.

Below are some weblinks to great websites, all designed to keep your child safe when online.

Simply by clicking on the links below you will be directed to specific information; or access the full website for lots of useful information.

Family activities around social media https://www.thinkuknow.co.uk/	THINK U KNOW .co.uk
Safety cards https://oursafetycentre.co.uk/	SAFETY CENTRE
Social media guides https://www.saferinternet.org.uk/	UK Safer Internet Centre
Starting a conversation about online safety https://www.nspcc.org.uk	NSPCC
Parent and carers toolkit https://www.childnet.com/	Childnet International

Other useful resources
CEOP - https://www.ceop.police.uk/safety-centre/
National Working Group (NWG) - https://www.nwgnetwork.org/for-parents/
Parents Against Child Exploitation (PACE) - https://paceuk.info/
Educate Against Hate (Advice on anti-radicalisation) - www.educateagainsthate.com/parents/

We hope you find the above information useful, if you have any questions, please don't hesitate to contact a member of staff.