

**St Bonaventure’s Catholic Primary School**

**Egerton Road,**

**Bishopston**

**Bristol,**

**BS7 8HP**

**Online Safety Policy 2024**

|  |  |
| --- | --- |
| **Policy Owner** | Headteacher |
| **Governing Body Committee** | Standards |
| **Issue Date** | 25.06.21 |
| **Last Review Date** | Term 3 2024 |
| **Next Review Date** | Term 3 2025 |

This policy is available at

<http://www.st-bonaventures.bristol.sch.uk/>

**Version History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Page** | **Description of Change** | **Origin of Change** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Vision**

*Striving to be the best we can, guided by the light of Christ.*

At St Bonaventure’s we are aware of the challenges and pressures put on children who have increasing access to online platforms, particularly post COVID-19. A school priority is to inform our children of the opportunities and potential risks of engagement online, and through focused teaching provide our children with the knowledge and tools to engage online healthily and safely.

**Rationale**

We have experienced increased rates of online safety incidents in upper KS2, and have observed behaviours which indicate that, particularly post COVID-19, our children have increased access to online platforms. Online safety incidents are having an increased impact on our children’s wellbeing and their relationships. Children have, generally, increased their screen time and proficiency with devices, which has increased the need for parental controls and risk management.

**Aims**

At St Bonaventure’s we aim to:

* Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
* Identify and support groups of pupils that are potentially at greater risk of harm online than others
* Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as ‘mobile phones’)
* Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

**The 4 key categories of risk**

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, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism.

Contact – being subjected to harmful online interaction with other users, such as child-on-child 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 – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and

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

**Legislation and guidance**

This policy is based on the Department for Education’s (DfE’s) statutory safeguarding guidance, [Keeping Children Safe in Education](https://www.gov.uk/government/publications/keeping-children-safe-in-education--2), and its advice for schools on:

* [Teaching online safety in schools](https://www.gov.uk/government/publications/teaching-online-safety-in-schools)
* [Preventing and tackling bullying](https://www.gov.uk/government/publications/preventing-and-tackling-bullying) and [cyber-bullying: advice for headteachers and school staff](https://www.gov.uk/government/publications/preventing-and-tackling-bullying)
* [Relationships and sex education](https://www.gov.uk/government/publications/relationships-education-relationships-and-sex-education-rse-and-health-education) – remove if not applicable, see section 4]
* [Searching, screening and confiscation](https://www.gov.uk/government/publications/searching-screening-and-confiscation)

It also refers to the DfE’s guidance on [protecting children from radicalisation](https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty).

It reflects existing legislation, including but not limited to the [Education Act 1996](https://www.legislation.gov.uk/ukpga/1996/56/contents) (as amended), the [Education and Inspections Act 2006](https://www.legislation.gov.uk/ukpga/2006/40/contents) and the [Equality Act 2010](https://www.legislation.gov.uk/ukpga/2010/15/contents). In addition, it reflects the [Education Act 2011](http://www.legislation.gov.uk/ukpga/2011/21/contents/enacted), 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 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 make sure all staff undergo online safety training as part of their annual child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email and staff briefings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will coordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

* Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
* Reviewing filtering and monitoring provisions at least annually;
* Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
* Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

* Ensure they have read and understand this policy.
* Agree and adhere to the terms on the Internet Code of Practice for staff and adults. (See appendix)
* Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures.
* Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a ‘one size fits all’ approach may not be appropriate for all children in all situations, and a more personalised or contextualized approach may often be more suitable.

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 (DSL)

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 the staff and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
* Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks.
* Working with the School Business Manager, SBM, to make sure the appropriate systems and processes are in place
* Working with the SBM and other staff, as necessary, to address any online safety issues or incidents.
* Managing all online safety issues and incidents in line with the school’s child protection and safeguarding policy.
* Ensuring that all online safety incidents are logged and dealt with appropriately in line with this policy.
* Ensuring that any incidents of cyberbullying are logged and dealt with appropriately in line with the school’s Relationship and Behaviour Policy.
* Updating and delivering staff training on online safety.
* Liaising with other agencies and/or external services if and when necessary.
* Providing regular reports on online safety in school to the staff and governing board.
* Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

The School Business Manager (SBM) and School IT Services

The SBM and School IT Services are responsible for:

* Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept 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 regular basis.
* Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

This list is not intended to be exhaustive.

All staff and volunteers

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

* Maintaining an understanding of this policy.
* Implementing this policy consistently.
* Agree and adhere to the terms on the Internet Code of Practice for staff and adults. (See appendix)
* Ensure all pupils adhere to the terms on the Internet Code of Practice for Pupils. (See appendix)
* Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing.
* Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes.
* Working with the DSL to ensure that any online safety incidents are logged on CPOMS 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 Relationship and Behaviour Policy.
* Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of ‘it could happen here’.

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 the Internet Code of Practice for Pupils.

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 the Internet Code of Practice for staff and adults.

**Educating pupils about online safety**

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

In Key Stage 1, pupils will be taught to:

* Use technology safely and respectfully, keeping personal information private.
* Identify where to go for help and support when they have concerns/worries about content or contact on the internet or other online technologies.

Pupils in Key Stage 2 will be taught to:

* Use technology safely, respectfully and responsibly.
* Recognise acceptable and unacceptable behaviour.
* Identify a range of ways to report concerns about content and contact.

By the end of primary school, pupils will know:

* That people sometimes behave differently online, including by pretending to be someone they are not.
* That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous.
* The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them.
* How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met.
* How information and data is shared and used online.
* What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context).
* How to respond safely and appropriately to adults they may encounter.

We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the internet and other technologies are embedded in our pupils’ lives, not just in our school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the internet brings.

* We will provide a computing, Jigsaw and Ten:Ten curriculum which educate the children about online safety.
* We will celebrate and promote online safety through a planned programme of assemblies and whole-school activities three times per year, including promoting Safer Internet Day each year. Class teachers will give children opportunities to explore their issues about keeping safe online in an age-appropriate way.
* We will discuss, remind or raise relevant online safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
* Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objective for specific curriculum areas.
* Pupils will be taught how to use a range of age-appropriate online tools in a safe and effective way.
* We will remind pupils about their responsibilities through an Internet Code of Practice which every pupil will be asked to sign.
* Staff will model safe and responsible behaviour in their own use of technology during lessons.
* We will teach pupils how to search for information and to evaluate the content of websites for accuracy when using them in any curriculum area.
* When searching the internet for information, pupils will be guided to use age-appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
* Pupils will be taught about the impact of online bullying and know how to seek help if they are affected by any form of online bullying.
* Pupils will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member.

**Staff use of school devices outside of school**

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

* Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol).
* Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device.
* Making sure the device locks if left inactive for a period of time.
* Not sharing the device among family or friends.
* Installing anti-virus and anti-spyware software.

* Keeping operating systems up to date by always installing the latest updates
* Work devices must be used solely for work activities.

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

**Staff 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 and staff briefings).

By way of this training, all staff will be made aware that:

 Children can abuse their peers online through-

* Abusive, threatening, harassing and misogynistic messages.
* Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups.
* Sharing of abusive images and pornography, to those who don’t want to receive such content.
* Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

* Develop better awareness to assist in spotting the signs and symptoms of online abuse.
* Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
* Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

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.

#

# Pupils using mobile devices in school

Pupils in UKS2 who walk home without a supervising adult may bring mobile devices into school, but are not permitted to use them during:

* School time (8.30-3.15)
* 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 Internet Code of Practice.

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

**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 our policies on Relationships and Behaviour policy and Internet Code of Practice. 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 and/or Staff 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 that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

**Monitoring and review**

The DSL and Computing leader will receive and respond to Prevent reports and investigate and respond as appropriate.

The DSL logs behaviour and safeguarding issues related to online safety.

Teachers are given access to laptops and the School Business Manager is responsible for maintaining records of who has been given which device.

Each child will be assigned a specific iPad; teachers are responsible for ensuring all children use their iPads and monitoring their use both visually and via the Classroom app. This ensures that online

incidents can be traced from IP address to a specific child. Children should never be given access to an adult’s computer or iPad.

This policy will be reviewed every year by the head teacher. At every review, the policy will be shared with the governing board.

**Links to other policies**

The following school policies should also be referred to:

* Child Protection and Safeguarding Policy
* Whistleblowing policy
* Relationship and Behaviour Policy
* Staff code of conduct
* Data Protection
* Curriculum Policy
* Computing Curriculum
* iPad Loan Agreement
* Home School Agreement

**Internet Code of Practice for KS2 Pupils**

We use computers and internet connection for learning and research.

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

* I will only use the internet when supervised by a teacher or adult.
* If I walk to/from school on my own and my parent has given me permission to bring my mobile telephone into school I agree to hand it in to the school office where it will be kept safe for me in a drawer in the office.  I will collect it at the end of the school day when I sign myself off the premises. I will not bring my phone into the classroom and I will not keep it in my bag.  I understand that the school does not accept responsibility for loss or damage of personal property.
* I will never tell anyone I meet on the internet my home address, my telephone number or my school's name without permission, or send a picture of myself. I will never arrange to meet anyone in person.
* I will never give any passwords to anyone, even my best friend, and I will log off when I have finished using the computer.
* I will never answer unpleasant, suggestive or bullying emails or messages and I will always report it to a teacher or parent.
* I will not look for bad language or inappropriate images and I will report bad language or inappropriate images to a teacher or parent if I come across them accidentally. I know that my teacher can check the websites I have visited!
* I will always be myself and will not pretend to be anyone or anything I am not. I know that the posting of anonymous messages and the forwarding of chain messages is not allowed.
* I understand that I can only use websites for my work in school and that I will not be allowed to use the Internet if I look at unsuitable material on purpose.
* I may not download **any** software from the Internet. I know that information on the Internet may not always be reliable and may need checking. I know that some web sites may be sponsored by advertisers.
* I will not use email to send or encourage material which is illegal, offensive or annoying or invades another person’s privacy.

✂ ----------------------------------------------------------------------------------------------------------------------------------

*I have read the Internet Code of Practice for Pupils document and I agree to support the school's policy.*

Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Class \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Internet Code of Practice for KS1 Pupils**

We use computers and the internet for learning.

These rules will help us to be fair to others. The will help keep everyone safe.

* I will only use the internet when I am near a teacher or adult.
* I will never tell anyone I talk to on the internet where I live or what my school is called, or send a picture of myself, unless a teacher or adult I know says it is okay. I will never say I will meet anyone in real life.
* I will never give any passwords to anyone, even my best friend, and I will log off when I have finished using the computer.
* I will never answer unkind messages and I will always tell a teacher or parent about it.
* I will not look for bad words or pictures and I tell a teacher or parent if I see them by accident. I know that my teacher can check the websites I have seen!
* I will always be myself. I will not pretend to be anyone or anything I am not.
* I know I can only use websites for my work in school. I will not be allowed to use the internet if I look at bad things on purpose.
* I will not use the internet to send things which are illegal, mean or annoying. I will not say things on the internet about other people unless they say it is okay.

✂ ----------------------------------------------------------------------------------------------------------------------------------

*I have read these rules. I agree to follow these rules.*

Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Class \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Internet Code of Practice for staff and adults**

Teachers/adults should be familiar with the school’s Online Safety Policy and the St Bonaventure’s responsible internet use guidelines for pupils.

Teachers should closely monitor and scrutinise what their pupils are accessing on the internet, including checking the history of pages. Computer monitor screens should be readily visible to the teacher, so they can monitor what the pupils are accessing.

Pupils should be given clear guidelines for the content of email messages and for sending and receiving procedures.

**Use of the iPads should be supervised by a teacher or adult. A list of which pupil uses which iPad shall be maintained and where possible adhered to by the teacher.**

Pupils should have a clearly defined focus for using the Internet and email. It is recommended that pupils do not use open forums such as newsgroups or chat rooms. Pupils should be taught skills and techniques to enable efficient and effective use of the Internet.

If offensive materials are found, the monitor should be switched off, any printed materials or disks should be confiscated and offensive URLs should be given to the Computing lead / IT Technician who will report it to Bristol CYPS. The incident should be reported to the Headteacher.

Virus protection has been provided by the school as viruses can be downloaded accidentally from the Internet. Pupils bringing work from home on data keys could also infect the computer - some viruses will format your hard drive!

Disciplinary action may be taken if the Internet is used inappropriately, for example, by accessing pornographic, racist or offensive material or for personal financial gain, posting photos of children, gambling, political purposes or advertising.

Software should not be downloaded from the internet (including screen savers, games, video clips, audio clips, \*.exe files) or installed by anyone other than an IT Technician or computing leader unless agreed with the computing leader in advance.

I have read the *Responsible Internet Use* document for pupils and teachers and I am familiar with the school’s policy on the use of the Internet, e-mail, the creation of web sites and network security.

I understand the insurance and care implications of any equipment loaned from school and agree to abide by the St Bonaventure’s Teacher’s Code of Practice.

✂ ----------------------------------------------------------------------------------------------------------------------------------

*I have read the Online Safety Policy and Code of Practice for Pupils. I agree to support the school's policy.*

Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_