St Bonaventure's Catholic Primary School
Egerton Road,
Bishopston
Bristol,
BS7 8HP

Online Safety Policy 2021

Policy Owner	Headteacher
Governing Body Committee	Standards
Issue Date	25.06.21
Last Review Date	20.10.21
Next Review Date	Term 6 2022

This policy is available at
http://www.st-bonaventures.bristol.sch.uk/

Vision

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. Our school priority is to inform our chidren of the opportunities and potential risks of engagement online, and through focussed 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 pervasive access to online platforms. Online safety incidents are having an increased impact on our children's wellbeing and relationships. Children have generally sufficiently 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
- 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:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

Relationships and sex education

Searching, screening and confiscation

It also refers to the DfE'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 programmes of study.

Legislation and guidance

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).

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.

The Designated Safeguarding Lead

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

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 headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged 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
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

School IT Services

The School's IT Service 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 termly basis

- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

The Computing lead

The Computing lead is responsibe for:

- Intregrating the online safety policy into the computing curriculum
- Ensuring that any online safety incidents are logged 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.

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
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use
- Working with the DSL to ensure that any online safety incidents are logged 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

Parents 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
- Parents can attend school events and use the recommended guidance on keeping children safe online.

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.

Educating pupils about online safety

New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter. St Bonaventure's Catholic Primary School endeavours to highlight benefits and risks of using technology and provides Safeguarding and education for users to enable them to control their online experience.

Links to other policies and national guidance

The following school policies and procedures should also be referred to:

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

The following local/national guidance should also be read in conjunction with this policy: PREVENT Strategy HM Government

- Keeping Children Safe in Education DfE September 2019
- Teaching Online Safety in Schools DfE June 2019
- Working together to Safeguard Children
- Learning together to be Safe: A Toolkit to help Schools contribute to the Prevention of Violent Extremism.

Teaching and Learning

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 well 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 Acceptable Use Policy which every pupil will sign

- School 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. See the Anti-Bullying Policy.

- 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, or an organisation such as Childline or the CEOP report abuse button.

Home Learning

- We will endeavour to ensure that pupils continue to receive a good level of education 'beyond the classroom' by providing a range of resources via our website and learning portals.

- We expect pupils to follow the same principles, as outlined in the school's Acceptable User policy, while learning at home.

- If a member of staff at our school communicates with pupils via Google Meet etc then it will be in accrodance with our Home Learning contingency Plan. Pupils must uphold the same level of behavioural expectations as they would in a normal classroom setting.

- Any significant behavioural issues occurring on any virtual platform must be recorded, reported and appropriate sanction imposed, which may include temporarily suspending access to group online learning. For all minor behavioural incidents, these should be addressed using the normal restorative approaches.

- Staff should be mindful that when dealing with any behavioural incidents, online, opportunities to discuss and repair harm will not be the same as if the child or young person was in school. Therefore, it may be necessary to have a discussion with the parents, regardless how minor the incident, to ensure the child is emotionally well supported.

- Children without a device are loaned one of the student iPads, which has all its contents wiped, and a management profile is installed to manage and monitor its use. We do not filter web content remotely; parents are responsible for the web contents which their children view while using the iPad at home.

For incidents in school or online:

- At every stage the child should be involved in or informed of the action taken
- Urgent or serious incidents should be referred straight to the DSL or deputy DSL
- If necessary, refer to the other related internal policies eg Anti-Bullying, Child Protection,
- Normal recording systems on CPOMS should continue. Entries should be factual and action/follow up recorded also.

Staff training, mobile devices, monitoring system

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including bullying, prejudice-based bullying and the risks of online radicalisation. Staff training will reflect the Safeguarding Action Plan, which will reflect online safety incident reporting and address the risks of the platforms our children are accessing.

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 meetings).

The DSL and deputy DSL 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.

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 Annual Safeguarding Action Plan.

How the school will respond to issues of misuse

The Internet Code of Practice is shared with children and parents each year and are required to agree to its rules.

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and record the incident and actions on our Online Safety Incident Form. 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 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.

Monitoring

The DSL and Computing leader will receive and repond to Prevent records and regular summaries; they invesigate and respond as appropriate.

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.

Review

This policy will be reviewed by the DSL, deputy DSL and Computing leader annually.

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 Teachers 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 _____

Home school agreement for loan of school iPad

The school will:

- loan the child a school iPad to access resources to support learning;
- pre-prepare the iPad with appropriate educational resources;
- ensure all iPads are wiped of data at the end of a loan period to ensure privacy of data is maintained;
- provide the child and parent(s), if required, with support in using the iPad and available resources.

The parent will:

- ensure that parental monitoring is enabled at home, via the parents'/guardians' internet provider, or the Screen Time feature in settings;
- attend online safety training provided by the school;
- return the iPad to the school when requested, usually at the end of an academic year;
- ensure the iPad is taken care of and returned to the school at the end of the loan period in the same condition with which it was issued;
- ensure their child does not exceed the recommended amount of screen time each day.

The child will:

- regularly use the iPad to help them with their learning;
- follow parents' rules for when and how long the iPad is used;
- keep the iPad in a safe place.