



Saint Benedict
A Catholic Voluntary Academy

Online Safety Policy

Date of Policy	September 2023
Author	Angela King
Review date	September 2024

Contents

1. Aims	3
2. Legislation and guidance.....	3
3. Roles and responsibilities.....	3
4. Educating pupils about online safety	5
5. Educating parents about online safety.....	6
6. Cyber-bullying.....	7
7. Acceptable use of the internet in school	9
8. Examining electronics devices.....	9
9. Staff using work devices outside school	9
10. How the school will respond to issues of misuse	10
11. Training	10
12. Monitoring arrangements	10
13. Links with other policies	11

1. Aims

Our school aims to:

1. Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
2. Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
3. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. 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 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.

3. Roles and responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the Head teacher to account for its implementation. The governing body 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 Father Jonathan Whitby-Smith. 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 1)

3.2 The Head teacher

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

Senior leadership team makes sure staff understand their roles, reviews the effectiveness of our systems and oversee reports

3.3 The Designated Safeguarding Lead

Details of the school's DSL and Safeguarding Team are set out in our child protection and safeguarding policy as well relevant job titles. The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Head teacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- DSL takes lead responsibility for filtering and monitoring reports and any safeguarding concerns that appear
- Ensuring that the filtering and Monitoring system in school is effective and is reviewed regularly
- Reviewing the online safety policy and 360 review tool annually
- Inform parents of online safety issues
- Ensuring that student learn about aspects of online safety in the curriculum and through safeguarding assemblies
- Working with the Head teacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Ensuring 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 logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety and filtering and monitoring
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Head teacher and/or governing board This list is not intended to be exhaustive.

3.4 The IT manager

The IT 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.

IT service provider has technical responsibility for maintaining and managing our system

- Conducting a full security check and monitoring the school's ICT systems on a monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy

ALL STAFF to be watchful and report any issues seen around school – either on computers, phones or overheard/ reported

- 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, which can be found here;

<https://www.stbenedictderby.srscmat.co.uk/wp-content/uploads/sites/25/2022/04/IT-Acceptable-Use-Policy-SRS-2022-1.pdf>

- Working with the DSL to ensure that any online safety incidents are 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.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Head teacher 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 (appendices 1 and 2) Parents can seek further guidance on keeping children safe online from the following organisations and websites which can be found on the safeguarding pages on the school website:
- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International

- Parent factsheet - Childnet International 3.7 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 1).

4. Educating pupils about online safety

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

In Key Stage 3, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns.

It is the aim of the Academy to ensure that by the end of secondary school, every pupil will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online

- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

The safe use of social media and the internet will also be covered in other subjects where relevant for example Key Stage 3 Computer Science curriculum. The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

5. 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 where there will be the opportunity for parents/carers to discuss online concerns and access support including technical guidance in helping to keep their children safe online. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Head of Year and or the DSL. Concerns or queries about this policy can be raised with any member of staff or the Head teacher.

6. Cyber-bullying

6.1 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.)

6.2 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. Form teachers will discuss cyber-bullying with their tutor groups, 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. This information is also available on the school website.

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.

6.3 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.

7. 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.

8. Pupils using mobile devices in school

Whilst pupils may bring a mobile phone in to school, we do not recommend or encourage it. Should they choose to so, it is on the understanding that they agree with the following limitations on its use, namely:

- Mobile phones must be switched off at all times during the school day, including break and lunchtimes, and remain off whilst pupils are on the school premises. It is not acceptable for phones merely to be put on silent mode. Failure to comply will result in confiscation.
- The phone must always be kept inside the pupils' school bag, and not be on their person such as inside their blazer pockets.
- No pupil may take a mobile phone into a room or other area where examinations are being held.
- The security of phone will remain the pupil's responsibility in all lessons including PE lessons
- If asked to do so, content on the phone (e.g. messages, emails, pictures, videos, sound files) will be shown to a teacher.

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. Details of the confiscation procedures in school can be found in the School's Behaviour Policy.

9. 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 the school's acceptable use policy.

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.

Any USB devices containing data relating to the school must be encrypted. 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.

10. 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 Student Acceptable Use 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 code of conduct policy.

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.

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

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. Incidents will be reported using CPOMS. This policy will be reviewed every year by the DSL. At every review, the policy will be shared with the governing board. The school 360 review will be reviewed

annually and there will be regular reviews of the school monitoring and filtering system with the Head of IT.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff Code of Conduct
- Data protection and freedom of information policy
- Complaints procedure
- SRS acceptable use policy