St. Bernadette's RC Primary School

E-Safety and Acceptable Use Policy

Revised: November 2024

Review: September 2026

E-Safety / Acceptable Use Policy

Jesus Christ is very important in our school. He is at the heart of everything we do. Our school is part of the mission of the church - making Jesus, known and loved. We try hard to live as Jesus wants us to, so that together we grow in faith, loving each other and loving God. We do all of these things because we want to keep Jesus among us every day at St Bernadette's.
"Together we Learn, Together we Achieve, Together we grow in God's love."

Introduction

Computing is an essential resource in the 21st century to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we need to build in the use of these technologies in order to arm our young people with the skills to access lifelong learning and employment. The Computing curriculum covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of IT within our society as a whole.

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web based resources, are not consistently monitored. All users need to be aware of the range of risks associated with the use of these Internet technologies.
At St. Bernadette's, we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

The purpose of this policy is to:

- Establish the ground rules we have in school for using the internet
- Describe how these fit into the wider context of our discipline and policies
- Demonstrate the methods used to protect children from sites containing inappropriate material, extremist views and violence.

Whole School Approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at this school:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-safety education programme for pupils, staff and parents

Roles and Responsibilities

E-Safety is recognised as an essential aspect of strategic leadership in this school and the Head teacher, with the support of the Governors, aims to embed safe practices into the culture of the school. The Head Teacher ensures that the policy is implemented and has ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named e-safety co-ordinators in our school from September 2024 are Mrs. Kay Mills (Head of School and Designated Safeguarding Leader) and Miss Saisha Kerr – Computing Subject Leader.
It is the role of the e-safety co-ordinator to keep abreast of current issues and guidance through organisations such as STOC Trust, Bury LA, LADO, DfE, CEOP (Child Exploitation and Online Protection), and Child Net. The e-safety co-ordinator ensures the Senior Management and Governors are updated as necessary.
All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.
All staff should be familiar with the school's policy including:

- safe use of e-mail
- safe use of the Internet
- safe use of the school network, equipment and data
- safe use of digital images and digital technologies, such as mobile phones, iPads and digital cameras
- publication of pupil information/photographs on the school website
- procedures in the event of misuse of technology by any member of the school community
- their role in providing e-safety education for pupils.

Staff are reminded/updated about e-safety regularly and new staff receive information on the school’s acceptable use policy as part of their induction.

Managing the school E-safety messages

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety policy will be shared with new staff, including the acceptable use policy as part of their induction.
- E-safety posters will be prominently displayed.

E-safety in the curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for safety guidance to be given to the pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety. E-safety will be taught under the guidance in the 2014 computing curriculum.

- We provide opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people’s information, images, etc through discussion, modelling, and activities as part of the ICT curriculum.
- Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies (see section on **Cyberbullying**)
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

Managing Internet Access

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

- Students will have supervised access to Internet resources through the school’s fixed and mobile internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

- Our internet access is controlled through Bury LA’s web filtering service.
- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety co-ordinator.
- It is the responsibility of the school, by delegation to the network manager, to ensure that antivirus protection is installed and kept up-to-date on all school machines.

Publishing pupil’s images and work

On a child’s entry to the school, all parents/guardians will be asked to give permission for their child’s photo to be taken and to use their child's work/photos in the following ways:

- on the school web site
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- in display material that may be used in the school’s communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the school
- general media appearances, e.g. local/ national media/ press releases sent to the press
- highlighting an activity (sent using traditional methods or electronically.)
- School Twitter account

Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
Pupils’ names will not be published alongside their image on any websites or the school Twitter account.
Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site.
Pupils will only have first names published on work in school. Staff will ensure that the following steps are taken in order to prioritise the e-safety of children.

- Ensure that permissions have been given and permission form has been signed before taking pictures of adults or children.
- Download images from camera/memory card/mobile device to the school secure shared area and store in a clearly labelled folder. This must be done within seven days.
- Delete original images on camera /iPads prior to them being taken off site.
- Prior to using images in other media (e.g. email, online, paper based and other collateral) ensure permission given covers intended use.
- Equipment must not be available for further use until images have been transferred or deleted.

Managing school devices

School equipment may only be used in school and not taken off site. If any equipment needs to be taken off site, it must be done so with permission from the Head Teacher or E-safety leaders. Devices are not to be used for personal use and must be left in school when requested, in order for essential updates to be applied.
If a device is lost, stolen or being used inappropriately it will be blocked in order to protect school and the safety of children.

Social networking and personal publishing

We block/filter access for pupils to social networking sites. Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils. Pupils will be advised never to give out personal details of any kind which may identify them or their location.

We realise that some of pupils will use social media outside of school, both pupils and parents will be provided with information on keeping safe in the social media arena. Pupils will be taught internet safety and etiquette to minimise the risk of exposing themselves to inappropriate attention.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not share with anyone, even friends. Staff and pupils are regularly reminded of the need for password security.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety rules.
- Users are provided with an individual network username
- Pupils are not allowed to deliberately access on-line materials or files on the school network, of their peers, teachers or others.
- If a password may have been compromised or someone else has become aware of the password the child or adult must report this to the e-safety co-ordinator
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks
- Individual staff users must also make sure that workstations are not left unattended and are locked.

Levels of security for data

Restricted	Protect	Public
Personal information related to pupils, staff (usually contained on the Management Information System)	School routines, schedules and management information	Display material around school and website and promotional materials

Responding to e-safety incidents/complaints

As a school we will take all reasonable precautions to ensure e-safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. Neither the school nor Bury LA can accept liability for material accessed, or any consequences of Internet access.

- Concerns relating to e-safety should be made to the e-safety co-ordinator. Any complaint about staff misuse must be referred to the Head teacher. Incidents should be logged and the Flowchart for Managing an e-safety Incident should be followed
- All users are aware of the procedures for reporting accidental access to inappropriate materials.
- The breach must be immediately reported to school's e-safety co-ordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety co-ordinator, depending on the seriousness of the offence; investigation by the Head teacher/ STOC Trust, LADO.
- Pupils and parents will be informed of the complaints procedure.
- Parents and pupils will need to work in partnership with staff to resolve issues.

Cyberbullying

Cyberbullying is the use of ICT, particularly mobile phones and the internet, deliberately to upset someone else. The whole school community has a duty to protect all its members and provide a safe, healthy environment. The Educations and Inspections Act 2006 states that Head teachers have the power 'to such an extent as is reasonable' to regulate the conduct of pupils when they are off site'. Although bullying is not a specific criminal offence in the UK law, there are laws that can apply in terms of harassing or threatening behaviour, for example, or indeed menacing and threatening communications.

There are many types of cyber-bullying. Here are some of the more common:

1. **Text messages** —that are threatening or cause discomfort - also included here is "bluejacking" (the sending of anonymous text messages over short distances using "Bluetooth" wireless technology)
2. **Picture/video-clips** via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.
3. **Mobile phone calls** — silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
4. **Emails** — threatening or bullying emails, often sent using a pseudonym or somebody else's name.
5. **Chatroom bullying** — menacing or upsetting responses to children or young people when they are in web-based chatroom.
6. **Instant messaging** (IM) — unpleasant messages sent while children conduct real-time conversations online using WhatsApp, Messenger or other 'chat' Apps
7. **Bullying via websites** — use of defamatory blogs (web logs), personal websites and online personal "own web space" sites.

Preventing Cyberbullying

It is important that we work in partnership with pupils and parents to educate them about Cyberbullying as part of our e-safety curriculum.
They should:

- understand how to use these technologies safely and know about the risks and consequences of misusing them
- know what to do if they or someone they know are being cyber bullied.
- report any problems with Cyberbullying. If they do have a problem, they can talk to the school, parents, the police, the mobile network (for phone) or the Internet Service Provider (ISP).

Additional online advice on how to react to Cyberbullying can be found on **www.kidscape.org** and **www.wiredsafety.org**

Supporting the person being bullied

- Give reassurance that the person has done the right thing by telling someone and inform parents.
- Make sure the person knows not to retaliate or return the message.
- Help the person keep relevant evidence for any investigation (taking screen capture shots, not deleting messages.)
- Check the person knows how to prevent it from happening again e.g. blocking contacts, or changing their contact details.

Investigating Incidents

All bullying incidents should be recorded and investigated in the St. Bernadette's Primary School bullying incident log. We will:

- advise pupils and staff to try and keep a record of the bullying as evidence
- take steps to identify the bully, including looking at the schools systems, identifying and interviewing possible witnesses, and contacting the service provider and police if necessary.

The police will need to be involved to enable the service provider to look into the data of another user.

Working with the bully and sanctions

Once the bully is identified, steps should be taken to change their attitude and behaviour by educating them about the effects of Cyberbullying on others. Technology specific sanctions for pupil engaged in Cyberbullying behaviour could include limiting or refusing internet access for a period of time. Factors to consider when determining the appropriate sanctions include:

- the impact on the victim: was the bully acting anonymously, was the material widely circulated and humiliating, how difficult was controlling the spread of material?
- the motivation of the bully: was the incident unintentional or retaliation to bullying behaviour from others?

Introducing the e-safety policy to pupils

- E-safety rules will be posted in all networked rooms, including in the Computing Curriculum and discussed with pupils at the start of each year
- Pupils will be informed that network and Internet use will be monitored.

Introducing staff to the E-safety policy

- All staff will be given the e-safety policy and its application and importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user and discretion and professional conduct is essential.
- Staff training in safe and responsible Internet use and on our e-safety policy will be provided as required.
- Teaching staff will be directed to be mindful of the teacher standards for professional conduct

Enlisting parents' support

At St. Bernadette's, we believe that it is essential for parents/ carers to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks. The school disseminates information to parents relating to e-safety where appropriate in the form of:

- Information evenings / Posters / Website postings / Newsletter items
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on school website)

Equal Opportunities - Pupils with additional needs

Staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities are planned and well managed for these children.

Parental Use of Social Media

Parents should be aware that social media and social forums are not a suitable platform for discussing school matters/grievances. Please see the School's Code of Conduct on Acceptable use of Social Media.

If you have concerns, which relate to school, please follow the school's grievance process:

Class Teacher

↓

Member of SLT

↓

Official Complaints Procedure

Reviewing this Policy

This policy will be reviewed on a yearly basis. It will encompass new technologies and developments. The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way. Staff, governors, parents and children (via our School Council) will be consulted on any changes.