'Living and Learning through Christ'

E-safety Policy

At St Bernadette Catholic Primary school Catholicity permeates all aspects of teaching and learning. Our values and beliefs aim to provide a strong level of coherence and focus which enriches the whole child. High standards are expected and articulated so that they are made explicit to all.

Scope

This policy applies to all members of St Bernadette Catholic Primary School (including staff, pupils, volunteers, parents / carers, visitors and community users) who have access to and are users of school IT systems, both inside and outside of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber- bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Objectives

The objectives of adopting an e-safety policy in our school are:

- to ensure that all members of St Bernadette Catholic Primary School community are aware of and build resilience in e-safety, in order to stay safe
- to raise awareness of the importance of e-safety in promoting the safeguarding and welfare of children and young people and vulnerable adults
- to increase everyone's understanding that e-safety is wider than just a technological issue
- to develop information, guidance, support and training in e-safety for key stakeholders including children, young people, vulnerable adults and their families
- to monitor, review and improve the e-safety strategy to ensure its impact and ongoing effectiveness.

Learning and Teaching

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 curriculum/Jigsaw curriculum/other lessons which has e-Safety related lessons embedded throughout.

We will celebrate and promote e-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day.

We will discuss, remind or raise relevant e-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.

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. 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 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.

Remote/Home Learning

Should the need arise, 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 Google classroom.

When our school/teachers communicate with pupils via google classroom, Zoom, Teams, Skype etc then it is important that this is only carried out with agreed approval. Pupils must uphold the same level of behavioural expectations, as they would in a normal classroom setting. This includes dressing appropriately when attending sessions remotely and ensuring there are no other distractions such as TV/radio/games consuls in the background.

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.

General Note for incident 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 head teacher, or a member of SLT.

If necessary, refer to the other related internal policies eg Anti-Bullying, Child Protection, ESafety etc

Normal recording systems on CPOMS should continue. Entries should be factual and action/follow up recorded also.

Staff Training

Our staff receive regular information and training on e-Safety issues, as well as updates as and when new issues arise. The code of conduct sets out expectations for staff.

As part of the induction process all staff receive information and guidance on the e-safety Policy and Safeguarding in relation to e-safety , All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.

All staff will be encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing ICT Systems and Access

The school will agree on which users should and should not have internet access and the appropriate level of access and supervision they should receive

All users will be made aware that they must take responsibility for their use and behaviour whole using the school ICT system and that such activity will be monitored and checked.

At Key Stage 1, pupils will access the network using an individual username and a class password which the teacher supervises.

At Key Stage 2, pupils will have an individual user account with an appropriate password which will be kept secure. They will ensure that they log out after each session.

All internet access will be undertaken alongside a member of staff or, if working independently , a member of staff will supervise at all times.

Members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID or password.

Managing Filtering

The school has the LA filtering system in place which is managed by the LA. Banned phrases and websites are identified.

The school has a clearly defined procedure for reporting breaches of filtering. All staff and pupils will be aware of this by attending the appropriate awareness training/online safety lesson

If staff or pupils discover an unsuitable site, it must be reported to IT technician/SLT immediately.

If users discover a website with potentially illegal content, this should be reported

immediately to teacher/SLT. The school will report such incidents to appropriate agencies including Internet Service Provider (ISP), Police, CEOP or the Internet Watch Foundation (IWF).

Any amendments to the school filtering policy or block and allow lists will be checked and assessed by the headteacher/IT technician and provider prior to being released or blocked.

The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-school requirement across the curriculum.

E-Mail

Staff and pupils should only use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.

Staff should not use personal email accounts for professional purposes, especially to exchange any school related information or documents or to email parents/carers.

Staff should not send emails to pupils unless it is part of google classroom remote learning provision. Parents should not use their child's google account to message teachers. They should use the teachers official work email.

Pupils are encouraged to immediately tell a teacher or trusted adult if they receive any inappropriate or offensive emails.

Irrespectively of how pupils or staff access their school email (from home or within school), school policies still apply.

Chain messages are not permitted or forwarded on to other school owned email addresses.

Social Networking

Staff will not post content or participate in any conversations which will be detrimental to the image of the school. Staff who hold an account should not have parents or pupils as their 'friends'. Doing so will result in disciplinary action or dismissal.

School social media sites should be password protected and run from the school.

Pupils Publishing Content Online

Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.

Pupils' full names will not be used anywhere on the website, particularly in association with photographs and video.

Parental agreement to share/publish photographs is secured at the point when the child starts school.

Pupils and staff must use school portable devices to store images/video/sound clips of pupils.

Mobile Phones and Devices General use of personal devices

Mobile phones and personally owned devices will not be used in any way during lessons or school time. Staff mobiles phones should always be switched off or in silent mode.

No images or videos will be taken on mobile phones or personally owned devices.

In the case of school productions, Parents/carers will be informed if they are permitted to take pictures of their child in accordance with school protocols and will be strongly advise

against the publication of such photographs on social networking sites.

The sending of abusive or inappropriate text, picture or video message is forbidden.

Pupils' use of personal devices

We discourage pupil mobile phones in years Reception to Year 5.

Year 6 pupil who need to bring a mobile phone in to school can only do so if the phone is placed in the secure storage at the start of the day and collected at the end of the day.

Pupils who do not follow the school policy relating to the use of mobile phones will not be permitted to bring their mobile phones into school.

Screening, Searching and Confiscation

The Education Act 2011, allows staff to lawfully search electronic devices, without consent or parental permission, if there is a suspicion that the pupil has a device prohibited by school rules, or the staff member has good reason to suspect the device may be used to:

- endanger the child or other children
- cause harm,
- disrupt teaching,
- break school rules,
- commit an offence,
- cause personal injury, or
- damage property.
- Any other issues

Staff use of personal devices

Staff are not permitted to use their own mobile phones or devices for contacting pupils or their families within or outside of the setting in a professional capacity.

Staff will not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use school provided equipment for this purpose.

If a member of staff breaches the school policy then disciplinary action may be taken.

Mobile phones and personally -owned devices will be switched off or switched to 'silent' mode, Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the senior leadership team in emergency circumstances.

CCTV

The school may use CCTV in some areas of school property as a security measure.

Cameras will only be used in appropriate areas and there is clear signage indicating where it is in operation.

General Data Data Protection (GDPR) and e-safety

Data must always be processed lawfully, fairly and transparently; collected for specific, explicit and legitimate purposes; limited to what is necessary for the purposes for which it is processed; accurate and kept up to date; held securely; only retained for as long as is necessary for the reasons it was collected.

GDPR is relevant to e-safety since it impacts on the way in which personal information should be secured on school networks, computers and storage devices; and the security required for accessing, in order to prevent unauthorised access and dissemination of personal material.

Staff need to ensure that care is taken to ensure the safety and security of personal data regarding all of the school population and external stakeholders, particularly, but not exclusively: pupils, parents, staff and external agencies.

Personal and sensitive information should only be sent by e mail when on a secure network. Personal data should only be stored on secure devices.

In the event of a data breach, the school will notify the appropriate body and Information Commissioner's Office (ICO).

Authorising Internet access

All staff must read and sign the code of conduct.

All parents will be required to sign the home-school agreement.

All visitors and students will be asked to read and sign the safeguarding notice on entry to the school.

Support for Parents

Parents attention will be drawn to the school's e-Safety policy and safety advice in newsletters, the school website, Facebook account and e-Safety information workshops.

The school website and Facebook account will be used to provide parents with timely and meaningful information about their children's school lives and work to support the raising of achievement. The website and F will also provide links to appropriate online-safety websites.

Radicalisation Procedures and Monitoring

It is important for us to be constantly vigilant and remain fully informed about the issues which affect the region in which we teach. Staff are reminded to suspend any professional disbelief that instances of radicalisation 'could not happen here' and to refer any concerns through the appropriate channels (currently via the Child Protection/Safeguarding Leads). Regular monitoring and filtering is in place to ensure that access to appropriate material on the internet and key word reporting it in place to ensure safety for all staff and pupils.

Sexual Harassment

Sexual harassment is likely to: violate a child's dignity, make them feel intimated, degraded

or humiliated and/or create a hostile, offensive or sexualised environment.

Online sexual harassment, which might include non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as 'sexting'; inappropriate sexual comments on social media; exploitation; coercion and threats).

Any reports of online sexual harassment will be taken seriously, and the police and Children's Social Care may be notified.

Responses to Incident of Concern

An important element of e-Safety is the ability to identify and deal with incidents of concern including the confidentiality of information. All staff, volunteers and pupils have a responsibility to report e-Safety incidents or concerns so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The school has incident reporting procedures in place and record incidents of an e-Safety nature on Cpoms.

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges, and in extreme cases, suspension or expulsion, in accordance with the school's Behaviour or Discipline Policy. The school also reserves the right to report any illegal activities to the appropriate authorities

We have carefully considered and analysed the impact of this policy on equality and the possible implications for pupils with protected characteristics, as part of our commitment to meet the Public Sector Equality Duty (PSED) requirement to have due regard to the need to eliminate discrimination, advance equality of opportunity and foster good relations.

Reviewed T2 November 2025	Next review T2 2027