St Bernadette's Catholic Primary School

Online Safety & Cyber Security Policy 2026- 27

Updated September 2026

Review date September 2027

This policy has been written in line with 'Keeping Children Safe in Education' 2025, 'Teaching Online Safety in Schools', statutory RSHE guidance and other statutory documents. Any issues and concerns with online safety must always follow the school's safeguarding and child protection procedures.

Context

What are the main online safeguarding risks?

At St Bernadette's over the past year, we have particularly noticed the following in terms of device use and abuse and types of online/device-based incidents which affect the wellbeing and safeguarding of our students:

- Unsupervised viewing of inappropriate videos by children in all year groups **at home**.
- Name-calling and falling out using WhatsApp outside of school by pupils in KS2.

Wider Context of risk

The Ofcom 'Children and parents: media use and attitudes report 2023' has shown that YouTube remains the most used site or app among all under 18s and the reach of WhatsApp, TikTok and Snapchat increased yet further. At St Bernadette's we recognise that many of our children and young people are on these apps regardless of age limits, which are often misunderstood or ignored. We therefore regularly remind about our children and our families about best practice in order to keep our children safe. Once something is seen or experienced, the harm is done and often cannot be unseen or undone.

20% of 3–4-year-olds have access to their OWN mobile phone, rising to over 90 percent by the end of Primary School, and the vast majority have no safety controls or limitations to prevent harm or access to inappropriate material. At the same time, 3- to 6-year-olds are being tricked into 'self-generated' sexual content (Internet Watch Foundation Annual Report) while considered to be safely using devices in the home and the 7–10-year-old age group is the fastest growing group for this form of child sexual abuse material, up 60 percent within 12 months to represent over 60,000 cases found (of this same kind where the abuser is not present).

In the past year, more and more children and young people used apps such as snapchat as their source of news and information, with little attention paid to the veracity of influencers sharing news. The 2023 Revealing-Reality: Anti-social-Media Report highlights that this content is interspersed with highly regular exposure to disturbing, graphic and illegal content such as fights, attacks, sexual acts and weapons. At the same time, the Children's Commissioner revealed that ever younger children are regularly consuming pornography and living out inappropriate behaviour and relationships due to 'learning from' pornography.

Ofcom report Children's online experiences

UK Safer Internet Centre - Useful information on current online issues

UK government report on online harm to children

Scope of this Policy

This Online Safety Policy sets out how St Bernadette's Catholic Primary school will safeguard members of our community online, in line with statutory guidance and best practice. The school is aware of the wider statutory requirements that informs this policy.

This policy applies to all members of the school community who access or use school digital systems, including staff, learners, governors, volunteers, parents/carers, visitors and community users. It applies to

use of school systems both on and off site, and to the use of personal devices on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the school, St Bernadette's Catholic Primary school will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school. Where these incidents are repetitive and take up an increasing amount of time or are of a criminal nature e.g. homophobic or racially motivated or include content which would constitute the sharing and distribution of nudes or semi-nudes or be classed as sharing of child pornography, it is likely that the Police will be informed along with any other relevant external agencies.

Purpose and Aims

This policy aims to promote a whole school approach to online safety by:

• Setting out expectations for all St Bernadette's community members' online behaviour, attitudes and activities and use of digital technology (including when devices are offline)

• To ensure our safeguarding team have a sound understanding and awareness of all elements of online safeguarding through effective collaboration and communication with technical colleagues (e.g. for filtering and monitoring), curriculum leads (e.g. HRSE) and external agencies.

• Helping all stakeholders to recognise that online/digital behaviour standards (including social media activity) must be upheld beyond the confines of the school gates and school day, regardless of device or platform, and that the same standards of behaviour apply online and offline.

• Facilitating the safe, responsible, respectful and positive use of technology to support teaching & learning, increase attainment and prepare children and young people for the risks and opportunities of todays and tomorrow's digital world, to survive and thrive online

• Helping school staff working with children to understand their roles and responsibilities to work safely and responsibly with technology and the online world:

- for the protection and benefit of the children and young people in their care, and
- for their own protection, minimising misplaced or malicious allegations and to better understand their own standards and practice
- for the benefit of the school, supporting our school mission, aims and objectives, and protecting the reputation of the school and profession

• Establishing clear structures by which online incidents will be treated, and procedures to follow where there are doubts or concerns (with reference to other school policies such as Behaviour Policy or Anti-Bullying Policy)

• Ensuring that, as an organisation, we operate in line with our Gospel Values and within the law in terms of how we use online devices. Always remembering the dignity of the person in all aspects of our online and offline interactions.

This policy applies to all staff, volunteers, children and anyone involved in activities with St Bernadette's Catholic Primary School.

This policy should be read alongside our policies and procedures on:

• Safeguarding & Child Protection Policy

• Behaviour Policy

• Anti-Bullying Policy

• Home School Agreement

• Code of Conduct Policy

• Social Media & Networking Sites Policy

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of the key legislation and guidance are available on:

- online abuse https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- bullying https://learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- child protection https://learning.nspcc.org.uk/child-protection-system/england

1. Introduction

At St. Bernadette's Catholic Primary School, we see technology as a vital area of development in all subjects and take significant steps to ensure that all staff and children have access to relevant, high quality technology. In many areas of work the use of technology is vital and must be protected from any form of disruption or loss of service. It is therefore essential that the availability, integrity and confidentiality of the technology systems and data are maintained at a level that is appropriate for our needs.
Online safety is a fundamental part of our curriculum at St. Bernadette's; it is a priority across all areas of the school. Our mission is to protect and prepare our children, staff, volunteers and members of a wider school community for the considerable breadth of issues associated with online safety, including but not limited to: -

• Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism;

• Contact: being subjected to harmful online interaction with other users; for example: peer to peer 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; for example, 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.

Online Safety

Online safety is an integral part of safeguarding and requires a whole school, cross-curricular approach. At St Bernadette's online safety provision includes:

Lead DSL/OSL who has responsibility for leading online safety. This includes:

- ❖ designing and implementing an online safety curriculum to address current needs and a curriculum which is responsive to individual needs
- ❖ Regular monitoring the online safety curriculum through pupil voice, book looks and learning walks to ensure all pupils (including for SEND and disadvantaged pupils) are being equipped with the knowledge and skills to stay safe online
- ❖ responsibility for internet filtering and monitoring
- ❖ recording and reporting to Governors on all aspects of Online Safety.

Curriculum - Teaching Online Safety using the cross-curricular framework 'Education for a Connected World – 2020 edition' from UKCIS (the UK Council for Internet Safety). Units are mapped to different curriculum areas and taught throughout the year using the Project Evolve resources. Online safety curriculum documents for each year group are available on the school website. This curriculum is further enhanced through the use of Purple Mash resources, Online Safety Day materials and activities and through St Bernadette's Pupil Development Plan.

Online Safety Champion - Mrs. Shoulder, the Headteacher, has the role of online safety champion, with the support of the online safety committee. Any problems, worries or concerns must be reported to her as soon as possible. If Mrs. Shoulder is not available, the next persons to report to are Mrs Round or Mrs Buchan (Our DSLs).

The role of the online safety Champion includes:

- ensuring that the policy is implemented and that compliance with the policy is actively monitored.
- ensuring that all staff are aware of reporting procedures and requirements should an online safety incident occur.
- ensuring an online safety Incident Log is appropriately maintained and regularly reviewed.
- keeping personally up to date with online safety issues and guidance through liaison with the Local Authority and through advice given by national agencies such as the Child Exploitation and Online Protection Centre (CEOP).
- providing or arranging online safety advice/training for staff, parents/carers and governors.

Online Safety Group - At St Bernadette's our Online Safety Group provides strategic oversight of online safety, monitors implementation and impact of the Online Safety Policy, and ensures online safety is embedded across safeguarding, curriculum and technical practice. It listens to and values staff, pupil and parent voice.

Membership

- DSL/ OSL - Mrs Shoulder
- SENDCo & Deputy Headteacher – Mrs Round
- Online Safety Governor- Mr Wyre
- IT/technical representative (internal or provider) - Mr Witts
- Learner representative(s) - Head Pupils

Core responsibilities

- The group supports the DSL/OSL to:

- Draft, review and monitor the Online Safety Policy and related documents.
- Oversee filtering and monitoring, including requests for change.
- Map and review online safety education for breadth, progression and relevance.
- Review anonymised incident data and technical logs to identify trends and emerging risks.
- Gather feedback from learners, staff and parents/carers and turn this into improvement actions.
- Promote learner voice, peer support and awareness activity.
- Track and evidence improvement actions.

Governance and impact

- Operates to agreed Terms of Reference (membership, frequency, reporting lines), reviewed annually.
- Coordinates with Safeguarding, Behaviour, Curriculum, Digital Strategy and Learner Voice as needed.
- Reports key themes, actions and impact to governors, and shares appropriate summaries with the wider community.

Parental & Family Engagement

Support - supporting and encouraging parents and carers to do what they can to keep their children safe online. At St Bernadette's, we do this through online safety information shared in our newsletters, assemblies and workshops.

Permissions - seeking parents' consent, through our Photograph Permissions Form, for photos / videos to be used in the school newsletter, on the website or shared externally. Photos or videos do not display the child's name unless this is for the local newspaper and parents' consent has been given. Class registers list children who do not have consent.

Whole school effort

- Age appropriate acceptable user agreements for **all** pupils and stakeholders.
- St Bernadette's Acceptable Use Agreements stresses the importance of online safety training and education and is intended to ensure that all users of technology in school (including staff, pupils, volunteers, parents/guardians & visitors who have access to school ICT systems) are responsible and are protected from potential risk in their everyday use of ICT for educational, personal and recreational purposes and reflects the content of the school's wider online safety Policy.
- Our AUP outlines the ways in which users are protected when using technologies, including passwords, virus protection, filtering and monitoring. Advice is provided for users on how to report any failings in technical safeguards.
- All staff, including visiting staff and other professionals, are expected to read, sign and adhere to our AUP.
- Pupils in EYFS and KS1 will be taught about the online safety rules which will displayed in each classroom and referred to when using technology. Parents will be expected to sign the AUP on their child's behalf.
- Pupils in KS2 will also be taught about the Acceptable Use Policy and expected to sign a copy. This will also be referred to whenever technology is used across the curriculum.

- In the event of technology being taken home, the parent and child will be made explicitly aware that the AUP is still in force. They will sign a disclosure to show they have read and understood the policy.

Incident Response

Clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child. All incidents are recorded and kept on file. Included in each report is the child involved and any others affected. What was seen/done and what were the next steps. Any subsequent actions are also recorded. These incidents are anonymised and used to effect school improvement.

Dealing with incidents - Any incidents are recorded by Mrs Shoulder and kept in the Online Safety File in her office. Decisions as to the course of action are discussed with SLT and any appropriate action is taken.

Illegal offences

Any suspected illegal material or activity is brought to the immediate attention of the Headteacher who will refer this to external authorities, e.g. Police, CEOP, Internet Watch Foundation (IWF). We never personally investigate, interfere with or share evidence as we may otherwise inadvertently be committing an illegal offence. It is essential that correct procedures are followed when preserving evidence to protect those investigating the incident. Potential illegal content is reported to the Internet Watch Foundation (http://www.iwf.org.uk). Examples of illegal offences are:

•Accessing child sexual abuse images.

•Accessing non-photographic child sexual abuse images.

•Accessing criminally obscene adult content.

•Incitement to racial hatred.

More details regarding these categories can be found on the IWF website http://www.iwf.org.uk

Inappropriate use

It is more likely that our school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with quickly and actions are proportionate to the offence. Some examples of inappropriate incidents are listed below with suggested sanctions.

Incident Procedure and Sanctions

- Accidental access to inappropriate materials by a child.
- Minimise the webpage/turn the monitor off.
- Tell the adult in charge.
- Persistent 'accidental' offenders will need further disciplinary action.
- Using other people's logins and passwords without permission, inappropriately and/or maliciously.
- Inform SLT or designated Online Safety Champion. Enter the details in the Incident Log.
- Additional awareness, raising of online safety issues with individual child/class.
- More serious or persistent offences will result in further disciplinary action in line with the Behaviour Policy.
- Deliberate searching for inappropriate materials.
- Bringing inappropriate electronic files from home.
- Using chats and forums in an inappropriate way especially outside school using personal mobile devices that may cause harm or distress to other children. ALL Staff are responsible for dealing with online safety incidents and reporting them to either Mrs. Shoulder or Mrs Round.

- Sanctions would be in line with those in the behaviour policy.
- Parents – Parents/carers must always be informed of online safety incidents involving their child(ren)
- Police will be informed where staff or children engage in or are subject to behaviour which is considered particularly concerning or breaks the law.

Forms of Online Abuse

Sexting

All schools should refer to the UK Council for Internet Safety (UKCIS) guidance on sexting (now referred to as Sharing nudes and semi-nudes: advice for education settings) to avoid unnecessary criminalisation of children. NB - where one of the parties is over 18, this is no longer sexting but child sexual abuse.

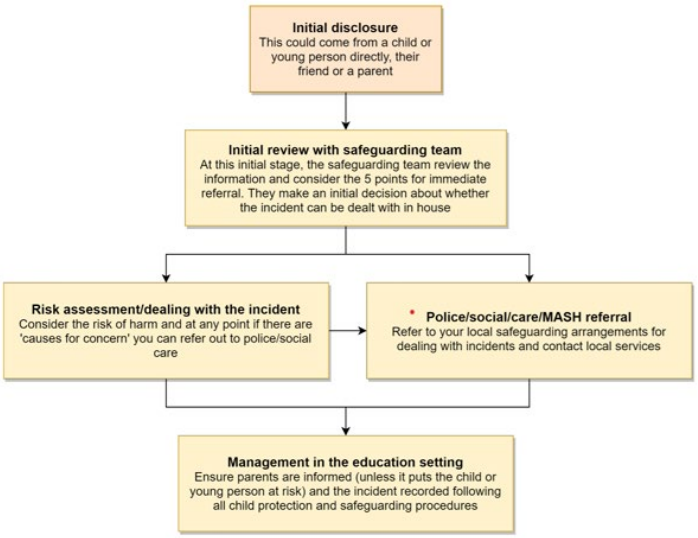
There is a one-page overview called Sharing nudes and semi-nudes: how to respond to an incident for all staff (not just classroom-based staff) to read, in recognition of the fact that it is mostly someone other than the designated safeguarding lead (DSL) or online safety lead to first become aware of an incident, and it is vital that the correct steps are taken.

Staff other than the DSL must not attempt to view, share or delete the image or ask anyone else to do so, but to go straight to the DSL. The school DSL will in turn use the full guidance document, Sharing nudes and semi-nudes – advice for educational settings to decide next steps and whether other agencies need to be involved.

***Consider the 5 points for immediate referral**

at initial review:

1. The incident involves an adult
2. There is reason to believe that a child or young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent (for example, owing to special educational needs)
3. What you know about the images or videos suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
4. The images involves sexual acts and any pupil in the images or videos is under 13
5. You have reason to believe a child or young person is at immediate risk of harm owing to the sharing of nudes and semi-nudes, for example, they are presenting as suicidal or self-harming



It is important that everyone understands that whilst sexting is illegal, pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Upskirting

It is important that everyone understands that upskirting (taking a photo of someone under their clothing, not necessarily a skirt) is now a criminal offence and constitutes a form of sexual harassment as highlighted in Keeping Children Safe in Education. As with other forms of child-on-child abuse pupils/students can come and talk to members of staff if they have made a mistake or had a problem in this area.

Bullying

Online bullying or cyberbullying, including incidents that take place outside school or from home, should be treated like any other form of bullying and our school Anti-Bullying Policy will be followed, including issues arising from 'banter'. More details can be found in our Anti-Bullying Policy

Child-on-child sexual violence and sexual harassment

Any incident of sexual harassment or violence (online or offline) should be reported to the DSL who will follow the full guidance in line with our Safeguarding Policy. Staff should work to foster a zero-tolerance culture and maintain an attitude of 'it could happen here'.

At St Bernadette's, we take all forms of sexual violence and harassment seriously, explaining how it exists on a continuum and that behaviours incorrectly viewed as 'low level' are treated seriously and not allowed to perpetuate. In the online environment, the recent proliferation of misogynistic content is particularly relevant when it comes to considering reasons for and how to combat this kind of behaviour.

Low-level Concerns Concerning Adults

The term 'low-level' concern does not mean that it is insignificant. A low-level concern is any concern – no matter how small, and even if no more than causing a sense of unease or a 'nagging doubt' – that an adult working in or on behalf of the school may have acted in a way that:

• is inconsistent with the staff code of conduct, including inappropriate conduct outside of work

and

• does not meet the harm threshold or is otherwise not serious enough to consider a referral to the LADO.

Examples of such behaviour could include, but are not limited to:

• not treating all children fairly and consistently in accordance with school policies
• humiliating children
• being over friendly with children
• having favourites
• taking photographs of children on their mobile phone, contrary to school policy, or
• engaging with a child on a one-to-one basis in a secluded area or behind a closed door.

If staff have a safeguarding concern or an allegation about another member of staff (including supply staff, volunteers or contractors) that does not meet the harm threshold, then this should be shared with the Headteacher. If your concerns relate to the Headteacher, you should raise them with a senior leader and the Chair of Governors.

Training:

- All staff undertake bi-annual online safety training
- All teaching staff undertake training on the use of AI in schools
- Annual Safeguarding training for all staff and Governors.

- Provide clear and specific directions to staff and volunteers on how to behave online through our induction process which includes the relevant policies listed at the start of this policy
- Provide support and training for all staff and volunteers on dealing with all forms of abuse, including child-on-child abuse, bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- Provide training for staff reporting concerns about adults to the Headteacher. If the concern is about the Headteacher, this is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).
- Training to include what to do if staff have concerns about the safeguarding culture or procedures, they should follow the Whistleblowing Policy. Useful names and numbers are included in the Safeguarding Posters in communal areas of the school.

Review:

- reviewing and updating our cybersecurity arrangements regularly to keep our information systems secure and ensuring staff have access to regular training
- completing an annual online safety audit and government's digital & technology standards, which involve a link governor, to review our approach and procedures
- examining and risk assessing any social media platforms and new technologies before they are used and with suitable training provided
- review any actions plans developed to address online incidents at regular intervals, in order to ensure that any problems have been resolved in the long term

Filtering & Monitoring:

- ensuring appropriate filters and monitoring systems are in place so that children cannot access harmful or inappropriate material from our school network
- Our school ensures that the infrastructure/network is as safe and secure as possible. We employ Centra Systems to support school use of technologies, subscribe to Lancashire County Council Education Digital Services and use Netsweeper to filter and monitor online usage, including Google searches. As part of the filtering and monitoring protection procedures in place, the Online Safety Champion (Mrs Shoulder), receives daily 'Suspicious Search Reports' and a weekly 'Full Monitoring Report' Any restricted searches are recorded and acted upon immediately.
  Where suspicious content is found the user will be traced back through their IP address and allocated equipment. The matter addressed as appropriate.
- All staff and governors receive regular training about filtering and monitoring and how they contribute to its effectiveness in keeping children and staff safe.
- Monitoring user activity on school devices is an important part of providing a safe environment for children and staff. Monitoring activities include:
  • physically monitoring by staff watching screens of users
  • pupils only permitted to use devices when supervised
  • devices numbered and allocated to pupils so that they can be traced by IP addresses
  • network monitoring using log files of internet traffic and web access

• senior leaders, with a governor if possible, carrying out specific checks of the filter and monitoring software – this must be done in pairs to safeguard the leader from allegations

Staff must report if:

• they witness or suspect unsuitable material has been accessed
• they can access unsuitable material
• they are teaching topics which could create unusual activity on the filtering logs
• there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
• they notice abbreviations or misspellings that allow access to restricted material
• devices used at home have been used to access inappropriate content

GDPR Security:

Security is a complex subject that involves all technology users in the school, dealing with issues regarding the collection and storage of data through to the physical security of equipment. The Lancashire Safeguarding Board online safety guidance is consulted to ensure that procedures are in place to ensure data, in its many forms, is kept secure within the school. In line with the requirements of the Data Protection Act, sensitive or personal data is recorded, processed, transferred and made available for access in school.

This data is:

- Accurate.
- Secure.
- Fairly and lawfully processed.
- Processed for limited purposes.
- Processed in accordance with the data subject's rights.
- Adequate, relevant and not excessive.
- Kept no longer than is necessary.
- Only transferred to others with adequate protection.
- Kept secure and staff are informed of what they can or can't do with data through this online safety Policy and the Acceptable Use Policy (AUP).
- Accessed by relevant staff who know the location of data or are aware of who to ask.
- Only used via approved means to access, store and dispose of confidential data.
- Not accessible without passwords.
- Backed up and secured via own class teachers such as reports, planning and assessment, etc. Staff are reminded about security through staff meetings and information on display in the staffroom.
- Ensure personal information about the adults and children at St Bernadette's, is held securely and shared only as appropriate.
- Access to Arbor (MIS System) must only be gained through devices which are provided by school. Staff are not permitted to access Arbor on Personal devices.

Staff & Pupil Email and Communication Systems

Staff must only use their Office 365 email account (@st-bernadettes.lancs.sch.uk) or Arbor for all school emails and messages. They must never use a personal/private email account (or other messaging platform)

to communicate with children or parents, or to colleagues when relating to school/child data, using a non-school-administered system.
Staff emails are monitored and may be read by the Headteacher or other person with delegated responsibility.
If messages need to be sent to parents, this can be done using the Arbor App for free. Arbor is centrally managed and administered by the school and they can be monitored/audited/viewed centrally; are not private or linked to private accounts).
This is for the mutual protection and privacy of all staff, pupils and parents, supporting safeguarding best-practice, protecting children against abuse, staff against potential allegations and in line with UK data protection legislation. Use of any new platform with communication facilities or any child login or storing school/child data must be approved in advance by the Headteacher and centrally managed. Any unauthorised attempt to use a different system may be a safeguarding concern or disciplinary matter and should be notified to the DSL (if by a child) or to the Headteacher (if by a staff member).
Where devices have multiple accounts for the same app, mistakes can happen, such as an email being sent from or data being uploaded to the wrong account. If this a private account used for communication or to store data by mistake, the DSL/DPO (the particular circumstances of the incident will determine whose remit this is) should be informed immediately.

To safeguard themselves, staff must:

- take care if/when accessing the school WI-FI
- do not join school WI-Fi on personal devices
- protect their usernames and passwords – do not share
- MUST not access personal emails on school devices / networks or school emails on personal devices
- take care when using your mobile or other personal device in school during breaks and not use personal devices to take photos.
- MUST not wear smart watches which can take photos or video

Pupil Emails

- Class email accounts for children are set up through Teams and are used to support remote learning and for communication with teachers.
- Online safety is adhered to, in particular, ensuring that children do not give any personal details and that a member of staff checks the content of any emails before they are sent. This is made clear before any emails are sent or received, through online safety lessons. Subject/email address/content of received emails is also be checked by a member of staff to ensure that children are not exposed to anything inappropriate. Children report anything inappropriate/unexpected to the member of staff immediately.
- Staff must report anything inappropriate/unexpected to Mrs. Shoulder. The BTLS filtering service should reduce the amount of SPAM (Junk Mail) received on school email accounts. Any incidents of Spam should be reported to BTLS.

Cyber Security

An increasing number of schools and colleges are being seriously impacted by cyber incidents: phishing attempts to steal money and passwords, or a ransomware attack that encrypts files preventing access. This

is because we hold lots of sensitive information which criminals can target to make money. Staff undertake regular cybersecurity training which highlights the common risks and measures they can take to keep safe. Top Tips Training | School Staff Training

• Powerful passwords - When implemented correctly, passwords are a free, easy and effective way of helping to prevent unauthorised users accessing devices or networks.

Staff are recommended to:

- ✓ Have a different password for each account / service. If this isn't possible then make sure your most sensitive accounts (e.g. access to student records) have a unique password.
- ✓ If you must write down your passwords, store them securely and away from your device.
- ✓ Consider using a password manager – or ask your IT team whether this is an option.
- ✓ Use two factor authentication (2FA) on sensitive accounts. This gives a way of double-checking you really are who you are claiming to be.
- ✓ Always lock your account when you step away or stop using your device, even if it's just for a
- ✓ minute. This applies in school or when working from home.

Passwords should be easy for you to remember but hard for somebody else to guess. We recommend that you don't include the following:

- ✘ Partner's, child's or pet's name
- ✘ Place of birth or favourite holiday destination
- ✘ Something related to your favourite sports team
- ✘ A list of numbers (e.g. 123456) or words like 'password' or 'qwerty

Watch out for phish!

In a typical phishing attack, scammers send fake emails to thousands of people asking for sensitive information (such as bank details) or containing links to bad websites. If in doubt, call it out – always ask for advice. When receiving an email you suspect of being a phishing email, ask yourself:

- ! Does it contain poor quality images of logos?
- ! Are there spelling or grammatical errors?
- ! Does it address you as 'dear friend' rather than by name?
- ! Is it asking you to act urgently?
- ! Does it refer to a previous message you don't remember seeing?
- ! Does the email address look suspicious?
- ! Does it ask you to download a file or click on a link?

• **USBs or Pen Drives** - USBs are a helpful way to move data but they can also spread viruses and malware from one computer or network to another. Staff are not permitted to use personal USBs or pen drives on school devices and for storing sensitive information. Staff are able to access the Staff Hub when working from home and therefore there should not be any need to use a USB.

Use of mobile devices

This includes all or any devices capable of Photographic, Audio and Video recording.

Mobile Devices Staff

All staff are allowed to bring in a mobile phone for personal use. During school session times, all phones should be set to silent mode and kept away out of sight. They must stay away during all of the school sessions throughout the day. Special permission may be sought and sanctioned by Mrs. Shoulder (the Headteacher) in certain circumstances, for example, during pregnancy, illness or possible medical emergencies. Pictures of children must never be taken on a mobile phone. Phones may be used during break times, out of the sight and hearing distance of children.

Teachers are not permitted to wear smart watches or any other devices such as glasses or pendants which have the capability to take photographs, audio or video in any circumstances.

Parents

Parents are politely requested to keep any mobile devices out of sight and refrain from answering any phone calls or using text messaging whilst inside the school building. They are also politely asked to show consideration to other parents and children whilst on school property. Parents are not allowed to take videos or photographs using their mobile devices (this includes smart glasses, pendants or other devices) on school property unless permission from Mrs. Shoulder (the Headteacher) has been granted. If visitors are suspected of making audio or visual recordings secretly and without permission, you may be asked to leave.

Activities outside the normal school day. (Sports Day, Shows, FOSB events)

Parents are asked to set their phone to silent mode or switch them off during any events and to show consideration to parents and children whilst on school property. Photographs and video footage can be taken of their own child under the Data Protection Act the as long as it is only of their child and for their own personal viewing only. Parents are reminded that they should not photograph or record in any way staff or other people's children without express permission. They must NOT post photographs or video footage of other children on social media sites under any circumstances. Under the Data Protection Act, parents are entitled to take photographs of their own children on the provision that the images are for their own use, e.g. at a school production. Including other children or for another purpose could constitute a potential breach of Data Protection legislation. Parents are not permitted to use any technologies that belong to the school.

Children

- Children are not routinely permitted to bring mobile devices to school. Children, in Years 5 & 6, who walk to school alone are permitted to bring a phone to school. The phone must be brought directly upon arrival, to the school office, where it will be kept secure until it is collected at the end of the day.
- Children are not allowed to take any videos, audio or photographs using their mobile devices on school property. This applies to after school, at any organised function such as the Summer Fair, School Discos or on Residential trips. If this does happen, it must be reported to Mrs. Shoulder (the Headteacher) as soon as possible. These incidents are likely to result in permission being revoked for your child to bring a mobile device to school and all videos, images or recordings will be deleted in the presence of the Headteacher.

- These rules are in place to remove the risks of online safety incidents and prevents children who would otherwise have free access to mobile phones and their data. These rules also prevent children, whilst at school, from sexually harassing their peers via their mobile and smart technology, sharing indecent images: consensually and non-consensually (often via large chat groups), and viewing and sharing pornography and other harmful content.

Other mobile devices & Smart Technologies

- **Staff and Parents are not permitted to bring in personal tablets, other mobile devices or smart devices.**
- School has a large number of Apple tablet devices available for staff and children to use for educational purposes. These iPads have restrictions and filtering (NetSweeper) in place to prevent children and staff from accessing iTunes, the apple store, changing settings, deleting and installing apps, sending email, using Facebook and using FaceTime. Age restrictions for apps and content have also been set up.
- These iPads are only to be used when fully supervised by an adult as part of a lesson or event and every iPad is allocated to a specific pupil or adult. Pupils and adults must only use the iPad which is allocated to them. Children are not permitted to use these devices to take photographs or video footage unless permission has been granted by the supervising adult. Any photos taken must be deleted at the end of the session and is the responsibility of the supervising adult. The iPads must be locked away when not in use. iPads are not to be used during wet break times.

Use of AI at St Bernadette's

St Bernadette's acknowledges the benefits of the use of AI in an educational context - including enhancing teaching and learning and outcomes, improving administrative processes, reducing workload and preparing staff and learners for a future in which AI technology will be an integral part.
Staff are permitted to use AI based tools to support their work where appropriate, within the frameworks provided below and are required to be professionally responsible and accountable for this area of their work.

- We will comply with all relevant legislation and guidance, with reference to guidance contained in Keeping Learners Safe
- We will provide relevant training for staff and governors in the advantages, use of and potential risks of AI. We will support staff in identifying training and development needs to enable relevant opportunities.
- We will ensure that, within our education programmes, learners understand the ethics and environmental impact of the use of AI and the potential benefits and risks of its use. The school recognises the importance of equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.
- As set out in acceptable use agreements, the school will use AI responsibly and with awareness of data sensitivity. Where used, staff should use AI tools responsibly, ensuring the protection of both personal and sensitive data. Staff should only input anonymized data to avoid the exposure of personally identifiable or sensitive information.

- Staff should always ensure AI tools used comply with UK GDPR and other data protection regulations. They must verify that tools meet data security standards before using them for work related to the school.
- Only those AI technologies approved by the school may be used. Staff should always use school-provided AI accounts for work purposes (Co-Pilot). These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- We will protect sensitive information. Staff must not input sensitive information, such as internal documents or strategic plans, into third-party AI tools unless explicitly vetted for that purpose. They must always recognise and safeguard sensitive data.
- The school will ensure that when AI is used, it will not infringe copyright or intellectual property conventions – care will be taken to avoid intellectual property, including that of the learners, being used to train generative AI models without appropriate consent.
- AI incidents must be reported promptly. Staff must report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to the relevant internal teams. Quick reporting helps mitigate risks and facilitates a prompt response.
- The school will audit all AI systems in use and assess their potential impact on staff, learners and the school's systems and procedures, creating an AI inventory listing all tools in use, their purpose and potential risks.
- We are aware of the potential risk for discrimination and bias in the outputs from AI tools and have in place interventions and protocols to deal with any issues that may arise. When procuring and implementing AI systems, we will follow due care and diligence to prioritise fairness and safety.
- The school will support parents and carers in their understanding of the use of AI in the school.
- AI tools may be used to assist teachers in the assessment of learner's work and identify areas for improvement. Teachers may also support learners to gain feedback on their own work using AI. Use of these tools should be purposeful, considered and with a clear focus on ensuring impact and understanding and mitigating risk
- Maintain Transparency in AI-Generated Content. Staff should ensure that documents, emails, presentations, and other outputs influenced by AI include clear labels or notes indicating AI assistance. Clearly marking AI-generated content helps build trust and ensures that others are informed when AI has been used in communications or documents.
- We will prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact-checked and reviewed for accuracy before sharing or publishing. This is especially important for external communication to avoid spreading misinformation.
- Recourse for improper use and disciplinary procedures. Improper use of AI tools, including breaches of data protection standards, misuse of sensitive information, or failure to adhere to this agreement, could be subject to disciplinary action.

Education & AI

Our school's educational approach seeks to develop knowledge and understanding of emerging digital technologies, including AI.

This policy outlines our commitment to integrating Artificial Intelligence (AI) responsibly and effectively within our school environment. We will use AI responsibly, safely and purposefully to support these aims:

- Enhance academic outcomes: Improve educational experiences and performance for pupils.
- Support teachers: Assist in managing workloads more efficiently and effectively.
- Educate on AI use: Promote safe, responsible, and ethical AI practices among staff and learners.
- Develop AI literacy: Incorporate AI as a teaching tool to build AI skills and understanding.
- Prepare for the future: Equip staff and pupils for a future where AI is integral.
- Promote educational equity: Use AI to address learning gaps and provide personalised support.

Our school's approach is to deliver this knowledge and understanding wherever it is relevant within the curriculum. This will include but is not limited to:

- Computing
- HRSE
- Cross curricular programmes
- Learning Support Programmes
- There will also be opportunities to enhance this knowledge through assemblies, online safety activities and to learn from external visitors.

Social Media

- Our school does not have any formal social networking accounts on any sites.
- Current popular examples of these sites are Facebook, Instagram and X. These sites provide users with simple tools to create a profile or page including basic information about themselves, photographs, and possibly a blog or comments. As a user on a Social Network site, you may have access to view other users' content, send messages and leave unmediated comments.
- Social Network sites are blocked by default through filtering systems used in our school, but these settings can be changed at the discretion of Mrs. Shoulder, the Headteacher.
- Whatever social media networks are used, individuals should always conduct themselves in a professional manner. If content is made available on the web it is available for everyone to see and potentially remains there forever.
- The content on Social Network sites may be unmediated and inappropriate for certain audiences.
- If a Social Network site is used personally by staff, they should pay close attention to the POLICY ON THE USE OF SOCIAL NETWORKING SITES AND OTHER FORMS OF SOCIAL MEDIA.
- Personal details must not be shared with children, and privacy settings must be reviewed regularly to ensure information is not shared automatically with a wider audience than intended. (See Mrs. Shoulder for support in this area.)
- They must not give personal contact details to pupils or parents/carers including mobile telephone numbers, details of any blogs or personal websites.
- Any content posted online should not:
  - × Bring the school into disrepute.
  - × Lead to valid parental complaints.

- Be deemed as derogatory towards the school and/or its employees.
- Be deemed as derogatory towards pupils and/or parents and carers.
- Bring into question their appropriateness to work with children and young people.
- Staff must not communicate with children using any digital technology, especially where the content of the communication maybe considered inappropriate or misinterpreted. Online Communications with parents, past pupils or siblings of pupils, especially if under the age of 18, is discouraged.
- Children, including, past pupils, must not be added as 'friends' on any Social Network site.
- Staff must not post inappropriate comments about staff or children that could be construed as instances of cyberbullying.
- Staff must not post images of children or adults on profiles without permission of the individuals involved, especially if the photographs contain children other than their own.

Instant Messaging

- These are all blocked through restrictions on the iPads or the Lancashire filter. Staff are made aware of the risks involved in using this technology, for example, viewing inappropriate images or making unsuitable contacts, through online safety meetings.
- Staff do not use school iPads for any personal communications.
- We do not allow any form of messaging through our website.
- Parents are contacted through Arbor. It is requested that any emails or texts sent are mentioned to Mrs. Shoulder, Mrs Round or Mrs. Maudsley in case parents/carers phone with any questions or concerns.

Virtual Learning Environment (VLE) / Learning Platform

- We use our own website and only staff have access and can access, modify or post things. Mrs. Shoulder is in charge of the website and has overall responsibility for its management, content and appearance. Mrs. Maudsley also supports Mrs. Shoulder with the website and has access to it.
- Our school website effectively communicates online safety to parents/carers through links to a variety of websites for advice and support. Also through displaying the online safety policy online, suggesting reading material, for example, the digital parenting website.
- Only relevant staff have the ability to update information on the website and regular meetings/discussions take place to ensure guidance is adhered to. Overall responsibility for the website belongs to Mrs. Shoulder, but responsibility for appropriate areas is delegated to relevant staff. Copyright is strictly adhered to and discussed with children as part of their online safety education. Any downloadable material is converted to the read-only format of PDF, where possible, to prevent content being manipulated and potentially redistributed without the school's consent.

Collaboration & Support

• actively seeking support from other agencies as needed (i.e. the local authority, LGfL, Mental Health Services, UK Safer Internet Centre's Professionals' Online Safety Helpline (POSH), NCA CEOP, Prevent Officer, Police, Nurse, IWF and Harmful Sexual Behaviour Support Service)

Monitoring and Review

Monitoring is the responsibility of the Headteacher, Governors (through the faith & Community Committee).

Any incidents will be reported termly to Governors by the Headteacher.

The policy will be reviewed annually.

The school is aware of our legal duties under the Equality Act 2010, to promote equality of opportunity and to reduce discrimination.