Policy: Online & Computer Safety Policy
Date: April 2025

Relevant supportive documents and legislation:

DfE: Keeping Children Safe in Education,

DfE: Preventing and tackling bullying

DfE: Searching, screening and confiscation at school.

DfE: protecting children from radicalisation: The Prevent Duty.

Education Act 1996 (as amended),

Education and Inspections Act 2006

Equality Act 2010. Education Act 2011

General Data Protection Regulations (GDPR) May 2018.

National Curriculum computing programmes of study.

This Policy Should be Read in Conjunction with the School's Remote Learning Policy

Links to other school policies and documents:

- Cyber Response Plan
- Child Protection and Safeguarding Policy
- Behaviour Policy
- British Values Policy
- Data Protection Policy
- Staff disciplinary procedures
- Data Compliance Plan (DCP)
- Privacy Notices

Date created: 27th March 2018 amendments approved March 2019 and Jan 2020, reviewed March 2021 & 2022, amended April 2023, April 2024, April 2025

Responsible: ICT Manager and Headteacher

Date Ratified: 16th April 2018

Responsible Committee: FGB under advice of Curriculum Lead Governors, GDPR Lead Governor and Safeguarding Lead Governor

Date to be reviewed: Annually

Statutory Policy: N

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- [Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will monitor online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure 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 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

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

3.3 The designated (and deputy) safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) are set out in our Child Protection and Safeguarding policy, as well as relevant job descriptions.

The DSL/Deputy DSLs takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Ensuring that any online safety incidents are logged (see appendix 4) 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 (appendix 3 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a monthly basis. Including a regular check on filtering, which will be logged.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Helping to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Helping to ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Administering password policies and encryption via BitLocker where appropriate.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) 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
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics

- Parent resource sheet – Childnet

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, where relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know
- The benefits of rationing time spent online, the risks of excessive time spent on electronic devices and the impact of positive and negative content online on their own and others' mental and physical wellbeing
- How to consider the effect of their online actions on others and know how to recognise and display respectful behaviour online and the importance of keeping personal information private
- Where and how to report concerns and get support with issues online

The safe use of social media and the internet will also be covered in other subjects where relevant.

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.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home and via the school website. This policy will be available to parents via the school website. Printed copies may be requested vis the school office.

Online safety will also be covered during Parents' Evenings and/or Parent Workshops.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher/DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

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.

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. Class teachers will discuss cyber-bullying with their classes, 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.

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 report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher / DSL / member of SLT.

- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL/Deputy DSLs immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial intelligence (AI)

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Copilot, and Google Gemini.

St Bernadette's recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

St Bernadette's will treat any use of AI to bully pupils in line with our Behaviour Policy.

St Bernadette's recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

To ensure that personal and sensitive data remains secure, no-one will be permitted to enter sensitive or personal data or any information that allows a child or colleague to be identified into generative AI tools or chatbots.

If personal and/or sensitive data is entered into a generative AI tool, St Bernadette's will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1 of the Data Protection Policy.

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.

More information is set out in the acceptable use agreements in appendices 1 and 2.

8. Pupils using mobile devices in school

Pupils may not bring mobile devices into school, unless arranged with the parents/guardians beforehand for reasons of personal safety and/or essential communication. In which cases the mobile device will be handed in to the School Office on arrival in the morning and collected at the end of the school day via the main entrance; ensuring the device does not travel through school.

Any mobile device found to be used by a pupil on the school site may trigger disciplinary action in line with the school 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 appendix 2.

Staff must ensure that their work device complies with UK GDPR regulations; ensuring that it is secure and encrypted with BitLocker. Staff must take all reasonable steps to ensure the security of their work device when using it outside school.

School will provide encrypted memory sticks for staff; personal memory sticks are not permitted. Staff must set a password in line with the guidelines set out in section 11. School Password Policy.

Work devices must be used solely for work activities.

VPN access allows secure and encrypted access to the school's SIMs and FMS server whilst offsite. Staff must only access the VPN at home on private Wifi connections and never in public, or a place where their activities can be witnessed. Any requests to use VPN away from a staff member's home must be made to the ICT Manager

Files now stored and access via onedrive and teams must not be shared via link or any other method to any external parties without permission from the school. Do not access cloud files using a personal device of any kind.

Access to the majority of school cloud services from countries outside of the UK will be automatically disallowed, including email. Please seek special permissions from ICT Manager or headteacher for this restriction to be temporarily restricted.

10. Use of Email and Electronic Communications and Printing

Children and Staff have access to the email system at St Bernadette's. Children's emails are monitored for inappropriate phrases and words, emails may only be sent internally to staff and each another within the St Bernadette's email system.

Staff must use the Email system exclusively for work purposes only. Email must not be stored or accessed on a personal device.

The photocopiers in school are protected with 'Papercut MF', a version of secure print, which forces all printing to be held by the photocopier until physically released with a personal code.

All staff must use Secure Print when printing sensitive information; if this is not available, staff must be stationed next to the destination printer when printing, and ensure all pages are immediately collected.

All documents are securely stored on the photocopier for 24 hours before being deleted automatically.

11. School Passcode and Password Policy

Passwords must be set for every electronic device abiding by the following rules:

- Children must have passwords to access the ICT equipment and websites, these must:
    - For KS1 accounts; be a minimum of 1 word with a number.
    - For KS2 accounts; be a minimum of one word, contain capital letters and numbers.

- Staff must ensure:
    - All school owned tablets and mobile devices have at least a 6-digit passcode. Seeking permission from ICT Manager or SMT should they wish to take a school device offsite.
    - Staff must set strong and unique passwords for all school accounts and equipment; a strong password is defined as below:
        - Containing at least 10 Characters
        - Containing at least three words or in the form of a sentence
        - Containing a number
        - Containing a capital letter

12. 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 the behaviour policy and/or Remote Learning 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 disciplinary procedures. 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.

13. 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 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.

14. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed Annually, initially by the ICT Coordinator, ICT Manager and Headteacher and then by the governing board.

Appendix 1: Acceptable Use Agreement (Pupils and Parents/Carers)

Rules for Responsible Internet Use for Pupils

- I will not give out my own details such as my name, phone number, school name or home address, unless my teacher/parents/carer gives me permission.
- I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will not send photographs or videos or any other information about myself to others without permission from my teacher/parents/carer.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my E-Safety.
- If I am given a password I never pass it on to anyone, even my best friend.
- I never hang around in an Internet chat room if someone says or writes something which makes me feel uncomfortable or worried, and always report it to my teacher/parents/carer.
- I never respond to nasty, suggestive or rude e-mails or postings in chat rooms/groups; I always report it to my teacher/parents/carer.
- I always tell my teacher/parents/carer if I see bad language or inappropriate things while I am online.
- I am always myself and do not pretend to be anyone or anything that I am not.
- I know that my school and the Internet service provider will check the sites I have visited.
- I understand that I will not be able to use the Internet at school if I deliberately misuse it.
- I understand that information on the internet may not always be reliable and sources may need checking.
- I understand that I am not permitted to use generative AI tools (such as ChatGPT, Copilot, Bard, Etc) or chatbots on school devices.

Pupil's Agreement

I have read and I understand the school Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times. (Parents are asked to read and explain the rules for responsible use with their children.)

Signed: _____ Class: _____ Date: _____

Parent's Consent for Computer Use and Internet Access

I have read and understood the school Rules for Responsible Internet use and give permission for my child to access the Internet. I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Signed: _____ Print Name: _____ Date: _____

Appendix 2: Acceptable use agreement (Staff, Governors, Volunteers and Visitors)

St Bernadette's Catholic Primary School

ICT Acceptable Use Policy

Teachers, Support Staff and Invited Guests

The school has provided computers for use by staff, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources and help to ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

This document outlines the care and procedures staff should take when using ICT, paying special attention to the directives and instructions specified within the UK General Data Protection Act (GDPR).

Please read this document carefully.

Equipment

- Always get permission before installing, attempting to install or storing programs of any type on the computers.
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment.
- Only use the computers for educational purposes.
- Personal devices may connect to the school Wi-Fi guest network only.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.
- Be aware and vigilant of viruses & malware, ensuring to occasionally run scans on equipment (including the school encrypted memory stick)
- If you suspect a virus, malware or hacking, please immediately contact the school's ICT Manager/Support.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Each laptop should be encrypted with BitLocker or equivalent encryption mechanisms, please ensure you have a "padlock" icon present and in the "unlocked" graphic on the C Drive:  . If this is not the case, please seek support from the ICT Manager immediately and refrain from using the computer outside of the school premises.
- Staff must never use unencrypted memory sticks.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or the school network at risk.
- Computer storage areas and USB sticks will be treated like school lockers. The ICT Manager, Data Protection Officer or members of the Leadership Team may review your files and communications to ensure that you are using the system responsibly.
- Camera's, iPads and other electronic devices must be securely locked away when not in use.
- Pupil and staff use of devices is monitored by both the filtering and monitoring software designed to alert the DSL when an inappropriate word is detected. Staff must supervise pupil equipment use.
- Under no circumstances is it permitted to enter sensitive or personal data or any information that allows a child or colleague to be identified into generative AI tools (such as ChatGPT, Copilot, Bard, Etc) or chatbots.

Password Policy and Access Security

- Passwords must be **strong** and **unique** for each and every login where individuals' data can be accessed. Examples of the latter include, but are not limited to:

- The computer login
- Subscription websites such as bugclub, professor assessor, mymaths, etc
- SIMS
- All other sites and programs which store identifiable and sensitive information.

A strong password is defined as: at least three words, a sentence, or a password made up of at least 10 characters, and must include a number and capital letter(s). eg. BlueSkyMorning14. DucksAtThePark18.

- Staff members must ensure that they use a different password for each system they use. E.g. SIMS password must be different from the computer login password. Passwords must not be used twice or repeated across different systems.
- Passwords that follow the guidelines of complexity and strength outlined in this document, will not have an enforced policy of change, as per the government guidelines specified here: https://www.ncsc.gov.uk/articles/problems-forcing-regular-password-expiry
- Staff must never leave a laptop unattended without first using CTRL + ALT + DELETE and Enter, to lock the computer.
- Passwords should not be shared. The only exception to this is if you feel it would help the ICT Manager to address IT issues relating to your school account/equipment.
- iPads and other tablets that are taken offsite must be secured by at least a strong 6 digit pin.
- Staff members should be aware that the password used to login to the school computer will also set the Email account password.

Saving Data

- Data residing on the school server or cloud will be split into several folders, and must be saved in the appropriate place on the server.
- These areas will be labeled by folder and accessible to staff who have been assigned permissions allowing their use.
- Please ensure data is saved to the correct areas **at all times**. Failure to do so may expose sensitive data to individuals who are not permitted access
- Ensure filenames are appropriately named and do not unnecessarily share data.

Home Access and Computer use outside of school

- Staff will be permitted to use their laptop at home or other private places for work purposes only. This includes access to the school network via the Virtual Private Network (VPN) under the following conditions:
  - Access must only be via the school computer; correctly configured and authorised by the school's ICT Manager and Headteacher/SLT.
  - The computer must be locked before leaving unattended for **any** amount of time.
  - School equipment must be used extremely vigilantly in public places, or where there is a risk that information could be incidentally or deliberately obtained, either by sight or through connections to unfamiliar networks. The VPN **should never be used on public** WiFi unless permission has been obtained from the ICT Manager or SLT beforehand.
  - Staff Shared and other files made available without a VPN are also available to you via Teams and Onedrive. Please do not access these files on a mobile or personal device (such as laptop, computer or otherwise) without permission from the school.

Printing

- Staff will be required to print all documents with any sensitive information to a photocopier with papercut MF enabled which enforces "Secure Print". Secure print prevents the document printing until the member of staff releases it with a private passcode.
- If Secure Print is not available on any photocopier, staff may print to an 'unsecured' printer, but extreme care must be taken. The member of staff must be stationed next to the destination printer when printing, and ensure all pages are immediately collected.

Discovering and reporting breaches of General Data Protection Regulation (UK GDPR)

Breaches of data where sensitive information has become obtained by unauthorized individuals (eg. In plain sight/ on an unlocked computer screen/document left on a printer) etc - must be reported to the Data Protection Officer immediately on discovery of the breach, in line with the schools Data Protection Policy.

It is the responsibility of all members of staff to be constantly vigilant to any breaches of data that may contravene the UK GDPR.

Internet

The internet as a resource is constantly changing. These guidelines will be updated in the light of experience and development of the internet itself.

- You should access the Internet only for school activities.
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.

Email & Calendar

St Bernadette's uses Office 365 to process and store Email. As a member of staff, you will have access to this resource. Please familiarise yourself with the following rules around school Email:

- Whenever an email is sent on behalf of the school it should include; the school's name, the sender's name, their job title and email address.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to the ICT Manager. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
- Emails should not be loaded onto any personal device.
- Any documents scanned for attachment purposes, must be deleted from the scan folder immediately after being sent.
- Always use your designated school email account for all school related business. Personal email accounts must never be used.
- If you receive an email erroneously sent and it contains sensitive information, please close the email as soon as this is realised and inform the sender immediately, delete and confirm deletion to sender.
- If you believe you have accidentally sent an email to the wrong person or person(s) containing sensitive information, then immediately inform the addressee urgently and instruct them to not read/share/or forward the email and delete immediately. Request confirmation from the recipient that these instructions have been adhered to. All such breaches should be immediately reported to the DPO.
- All email attachments containing sensitive information should be password protected/encrypted with a strong password. The password should be communicated to the recipients verbally where possible, otherwise by a follow up email containing only password.
- Do not include sensitive information with the email body. Ensure this is contained in the attachment only.
- Emails containing sensitive information should not be sent to parents or the public under any circumstances. Please see the school office for communicating such information to parents.
- Internal emails should be void of all sensitive information as far as possible, when needing to include such information, please refer to the location on the school's file server instead of attaching/including in the body of the email.

Social Networking sites

Social media applies to blogs, microblogs such as Facebook, Twitter, Bebo, Linkedin, Videos, social networks, discussion forums, wikis and other personal webspace.

- Social media should not be accessed on the schools premises, with the exception of those with the responsibility of maintaining the school's social media presence on the designated school device
- Do not speak for the school unless you have express permission to do so, this covers all comments relating to the school
- If you can be linked to the school, act appropriately. This include photos and status updates
- Remember that colleagues, prospective employers, parents and children may see your online information
- You should not be 'friends' with any pupils from our school. Unless there are exceptional circumstances, eg child or sibling
- Please choose your 'friends' carefully, especially in light of the above.
- Ensure your settings are on private and only you and YOUR friends can see them
- If in doubt please seek advice from the school

Disciplinary Action

Disciplinary action may be taken against employees who contravene these guidelines. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the school's acceptable use policy and agree to use the school's computer facilities within these guidelines.

Name: _____ Signature: _____

Date: _____

Appendix 3: online safety training needs – self-audit for staff

Online safety training needs audit	
Name of staff member/volunteer:	**Date:**
Do you know the name of the person who has lead responsibility for online safety in school?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training? Please record them here.	

Appendix 4: online safety incident report log

St Bernadette's Catholic Primary School

Incident No:

E-Safety Incident Report

Date of Incident:	Location of Incident:

Name of person who discovered / identified incident:
Name(s) of Individual(s) involved:

Brief description of incident:
Brief description of any action taken at time of discovery:

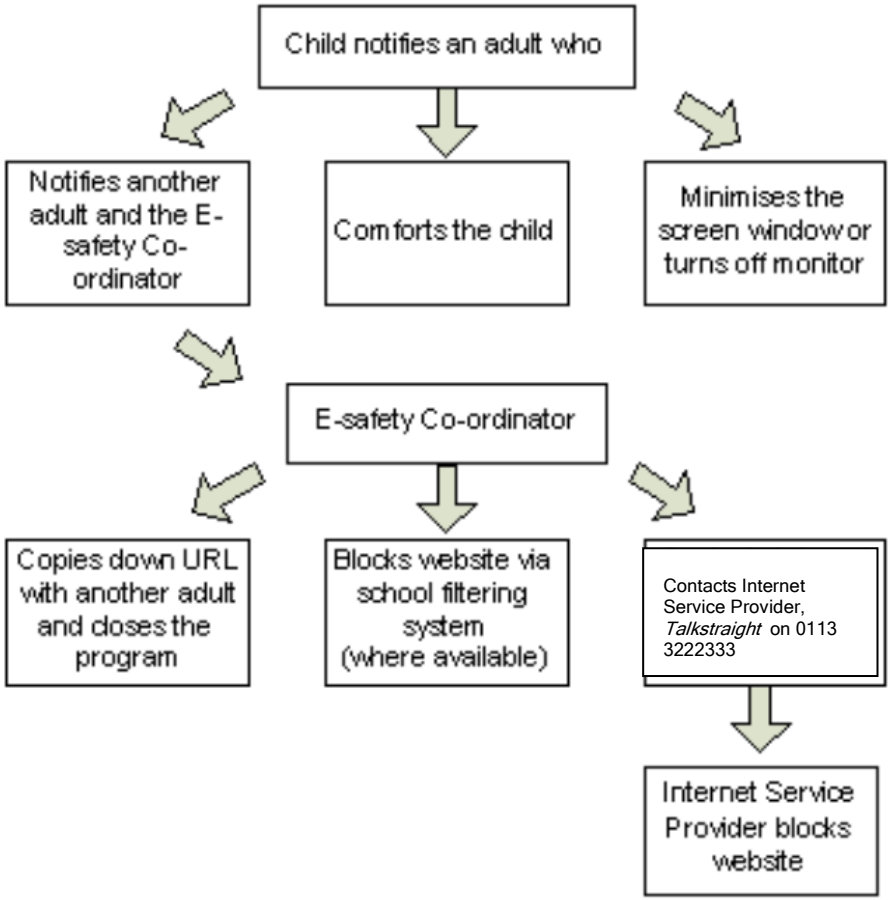
Comments / Notes

Date form sent to Headteacher / ICT Manager	Signature

Appendix 5: E-Safety Reporting Procedure

St Bernadette's Catholic Primary School E-Safety Reporting Incidents

E-safety Incident – View of Inappropriate Material



E-safety Incident – Receipt of an Abusive Email or Message