St. Bernadette's Catholic Primary School

Acceptable Use Policy
2026 2027

At St. Bernadette's Catholic Primary School, you will find us caring, hardworking and co-operative. We follow the ways of Jesus using our talents and gifts to make our school special. We show respect to all and welcome you.

Policy owner	Mrs Kidner
Named senior leader	Miss Finnegan
Updated	September 2026
Review date	September 2027, or sooner following change in guidance
Policy status	Computing, online safety and digital policies
Publication	SharePoint; hard copy available on request

Rationale

This policy sets out the school's expectations for the safe, responsible, lawful and professional use of technology, digital systems, email, internet access, social media, mobile devices, images and artificial intelligence. It should be read alongside the Safeguarding and Child Protection Policy, Online Safety Policy, Staff Code of Conduct, Data Protection Policy and Staff Handbook. The policy applies current safeguarding, data-protection, copyright and cyber-security expectations to day-to-day practice at St. Bernadette's Catholic Primary School.

- Copyright, Designs and Patent Act (1988)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Data Protection Act (2018)
- UK General Data Protection Regulation (GDPR)
- Data (Use and Access) Act 2025
- Keeping Children Safe in Education (2026)

PART 1 - INTRODUCTION

1.1 Purpose

This is a statement of good computer practice to protect St. Bernadette's from casual or intentional abuse. With the growth in use of email and access to the Internet throughout the organisation, there are a number of threats and legal risks to the school, as well as the potential costs of time wasting, that can be avoided by following the practice outlined.

Although both these tools are provided first and foremost for business use, St. Bernadette's accepts that on occasion they may be used for personal use. At all times users should take into account these guidelines and adhere to them.

1.2 Scope

These guidelines apply to all employees who have access to the Internet and other communication technology, or digital and information and communication tools for educational, recreational and personal use.

1.3 Publicising the guidelines

Effective communication is vital to increase staff awareness of these guidelines and their use within St. Bernadette's. All users will be notified of the Acceptable Use Policies for Email and the Internet to which these guidelines refer.

In addition, all such policies and guidelines will be available on the school network.

Further, new starters should not be given access to email or the Internet until they have seen and accepted these policies. This will be the responsibility of their line manager.

Any major revisions to these policies or guidelines will be notified to staff at staff meetings.

1.4 Monitoring

The school operates filtering and monitoring systems across school-managed networks and devices to help protect pupils, staff and school information from illegal, inappropriate or harmful online content and activity. Operational arrangements, including the school's managed monitoring provision, escalation routes and assurance checks, are set out in the Online Safety Policy.

Monitoring is proportionate and undertaken for safeguarding, cyber-security, legal and operational purposes. Users should understand that activity on school systems, accounts and devices may be monitored, reviewed and recorded in accordance with school policies and applicable law.

Filtering and monitoring systems will be reviewed at least annually to ensure that they remain effective and appropriate to the school's safeguarding needs, including consideration of emerging technologies and AI-related risks.
The review will include checks that filtering and monitoring work appropriately across school-managed internet-connected devices and relevant locations. Records of checks, findings and actions will be maintained.

The Designated Safeguarding Lead (DSL), the appropriate member of the Senior Leadership Team and IT support will work together to ensure that filtering and monitoring arrangements are effective, that roles are clearly understood and that concerns are acted upon appropriately.
All staff must understand the school's filtering and monitoring arrangements and know how to report inappropriate or harmful online content or activity.

Any safeguarding concern identified through filtering or monitoring must be reported to the DSL or Deputy DSL in accordance with the school's safeguarding procedures.

1.5 Disciplinary Process

Breaches of this policy may be managed under the school's disciplinary procedures and, where appropriate, safeguarding, data-protection, cyber-security or criminal procedures. Serious or deliberate misuse, including accessing, creating, storing or distributing illegal or harmful material, may constitute gross misconduct and may lead to referral to the DSL, LADO, police or another relevant authority as appropriate.

PART 2 - RESPONSIBILITIES

2.1 Governors and Senior Leadership Team.

The policies and these guidelines have been approved and adopted by the Governors and Senior Leadership Team.

2.2 St. Bernadette's

St. Bernadette's will ensure that users are notified of their responsibilities with regard to the use of email and the Internet. If children are using a shared user account, teachers will assign children specific computer and laptop numbers for monitoring purposes. Through the use of 3rd party "firewall" software, St. Bernadette's will monitor Internet and email use. Also, the appropriate security virus

prevention mechanisms will be maintained and updated to meet the ongoing requirement of the school.

2.3 Employees

All staff with access to email, the Internet or other digital systems are responsible for complying fully with this policy and the school's wider safeguarding, online safety and data protection policies.
Staff must:

- use school technology and digital systems responsibly and professionally;
- understand and follow the school's filtering and monitoring arrangements;
- report inappropriate, harmful or concerning online content or activity;
- report safeguarding concerns relating to online activity to the DSL or Deputy DSL without delay;
- protect passwords, devices and confidential school information from unauthorised access;
- lock their device whenever they leave it unattended, even for a short period, and must log off or shut down the device when it is no longer required, particularly at the end of the working day
- use school-approved systems and applications when handling school or pupil information;
- use artificial intelligence responsibly and in accordance with Part 9 of this policy; and
- complete relevant online-safety and filtering and monitoring training provided by the school.

PART 3 - EMAIL GUIDELINES

3.1 Personal Use

Employees are permitted to send personal emails on a limited basis (but not within directed time - 8.30am – 3.30pm) as long as this does not interfere with their job responsibilities. It should be noted that any email messages are not guaranteed to be private and remain the property of St. Bernadette's School.

When using a portable device, emails should only be accessed using the Microsoft 365 Outlook app.

3.2 Confidentiality

School email is a professional communication system. Messages may form part of the school's official records and must be written, stored, shared and retained in accordance with the school's Data Protection Policy, Records Management arrangements and professional standards. Confidential, personal or special-category information must only be shared where there is a lawful and necessary reason and using school-approved secure methods.

Emails containing sensitive information should be protected appropriately, including encryption where required. Staff must check recipients carefully and use Bcc where appropriate when sending messages to multiple external recipients.

When responding to parents/carers, staff must use school-approved email accounts and communication channels. School email use may be monitored, reviewed and recorded for safeguarding, security, compliance and operational purposes; users should not assume that use of a school account is private. In some instances, where the nature of a message may be deemed confidential, it may be appropriate to notify, or even seek permission from, the original sender before forwarding a message onto another

recipient.

3.4 Dissemination of Information
In cases where information of a general nature is circulated via email or on an electronic notice board, database or web site, it is the responsibility of the creator to ensure that members of their staff who do not have access to the system are notified of the information.

3.5 Inappropriate behaviour
Users should not send messages that contain any unsuitable material or defamatory statements about other individuals or organisations.

Messages should not contain material or language that could be viewed as offensive to others or as contravening St. Bernadette's Equal Opportunities Policy, N.B. what may appear appropriate to one person might be misconstrued by an other.

3.6 Canvassing, lobbying, advocacy or endorsement
Material, which could be construed as canvassing, lobbying, advocacy or endorsement should not be sent by email, particularly if this is commercially- or politically- based, and more particularly if this expresses a personal, rather than a school, view.

3.7 Virus Protection
To prevent the risk of potential viruses, users should not open any unsolicited email attachments or independently load any software, including screensavers, onto their computers. If a user does inadvertently open a message or attachment that contains a virus, they need to contact the IT co-ordinator or school technician immediately and close the message and attachment. It should not be accessed again without approval.

In some instances it might be appropriate to inform the original sender that their message contained a virus.

3.8 Security
All staff with access to email, the Internet or other digital systems are responsible for complying fully with this policy and the school's wider safeguarding, online safety and data protection policies.
Staff must:

- use school technology and digital systems responsibly and professionally;
- understand and follow the school's filtering and monitoring arrangements;
- report inappropriate, harmful or concerning online content or activity;
- report safeguarding concerns relating to online activity to the DSL or Deputy DSL without delay;
- protect passwords, devices and confidential school information from unauthorised access;
- use school-approved systems and applications when handling school or pupil information;
- use artificial intelligence responsibly and in accordance with Part 9 of this policy; and
- complete relevant online-safety and filtering and monitoring training provided by the school.

3.9 Housekeeping

Staff should manage email and files responsibly, deleting material that is no longer required and retaining or archiving records in accordance with the school's retention arrangements. Large files should be shared using approved school systems rather than unnecessary mass email attachments.

PART 4 - INTERNET GUIDELINES

4.1 Rules for professional use

Internet access is provided through school-managed systems and is subject to the school's filtering and monitoring arrangements. Users must use school-approved software, services and websites for school business and must not download or install unapproved software, browser extensions, applications or files. Any software used by the school must be appropriately licensed, secure and approved through the school's IT arrangements.

4.2 Personal use

Limited personal internet use may be permitted in staff-only time and areas where it does not interfere with professional duties, safeguarding responsibilities or the operation of the school. Personal use remains subject to this policy, filtering, monitoring and professional conduct expectations.
School systems may monitor and record internet use for safeguarding, cyber-security, legal and operational purposes. Users should not assume that activity on school networks, accounts or devices is private.

4.3 Respecting copyright

Users must respect copyright, licensing and intellectual-property rights. Staff must not download, copy, reproduce or distribute material where they do not have permission or a lawful basis to do so. Unlicensed software must not be installed or used.

4.4 Security

Users must protect school systems and confidential information. They must use their own authorised accounts, keep passwords and authentication methods secure, lock devices when unattended and never attempt to bypass security, filtering or monitoring controls. Suspected cyber-security incidents, phishing, malware, lost devices or unauthorised access must be reported promptly to the ICT Operations Manager and, where relevant, the DSL or Data Protection Lead.

4.5 Malware and cyber security

School devices are protected by technical security measures, but users must remain alert to malicious links, attachments, downloads and requests for credentials. Staff must not open suspicious attachments or install unapproved software and must report suspected phishing, malware or compromise immediately.

4.6 Inappropriate or harmful content

Users must not deliberately access, create, store or distribute illegal, inappropriate or harmful material. This includes, but is not limited to, child sexual abuse material, pornography, extremist content, material promoting self-harm or suicide, hateful or discriminatory content, or other material that presents a safeguarding risk. If harmful or illegal content appears inadvertently, staff should stop the activity, preserve any necessary evidence without forwarding or copying the material, and report it immediately to the ICT Operations Manager and DSL in accordance with safeguarding procedures.

PART 5 – SOCIAL NETWORKING SITES

The school recognises that staff may use social media, messaging services and other online platforms personally and professionally. Staff must maintain professional boundaries, confidentiality and safeguarding standards at all times, including outside working hours.

General expectations for social media and online communication:

- Staff must not contact, friend, follow or privately message current pupils through personal social media, messaging apps, personal email accounts or personal telephone numbers.
- Staff should use appropriate privacy and security settings, while recognising that no online content can be guaranteed to remain private.
- Staff must not publish personal, confidential or safeguarding information about pupils, families, colleagues or the school through personal accounts.
- Staff should remember that screenshots, sharing, search tools and platform features can make information visible beyond the intended audience.
- Staff must not disclose confidential or sensitive information about pupils, families, colleagues or school business.
- Only authorised staff may publish on official school websites or social-media accounts or communicate publicly on behalf of the school.
- Staff must not post content that could reasonably compromise safeguarding, professional boundaries, confidentiality or the reputation of the school or profession.
- Staff must never post images, recordings or information about pupils from personal accounts or personal devices.

Staff Profiles

5.1 Statuses/comments

- Staff must not post comments or material that could reasonably bring the school, pupils, families, colleagues or the profession into disrepute.
- Pupils, families or confidential school matters must not be identified or discussed through personal social-media accounts.
- Staff should consider the privacy and professional boundaries of colleagues before naming, tagging or posting images of them.

5.2 Photos/videos

- Staff must ensure that personal photographs or videos do not breach confidentiality, safeguarding expectations or professional standards.
- Staff should obtain permission before posting photographs or recordings of colleagues and should respect any request not to be included.
- Privacy settings should be reviewed regularly, but staff should assume that anything posted online may ultimately become public.

Contact with pupils

5.3 Connections with pupils, parents and former pupils

- Staff must not accept or initiate social-media connections with current pupils.

- If a current pupil attempts to contact or connect with a member of staff through a personal account, the member of staff must not engage and should report the contact to the DSL/DDSL in accordance with safeguarding procedures.
- Staff should avoid personal social-media relationships with parents/carers where these could blur professional boundaries. School-related communication must use approved school channels.
- Contact with former pupils should be considered carefully in light of age, safeguarding, professional boundaries and any continuing connection with the school. Staff must not establish personal online contact with former pupils who are still children where this could compromise professional boundaries.

5.4 Messages

- Staff must not privately message current pupils through social-media or messaging platforms, even for school-related purposes. School communication must use approved systems.
- If a member of staff receives a private message from a pupil, they should not reply through the personal account. They must retain and report the contact to the DSL/DDSL, who will decide the appropriate safeguarding response and whether parents/carers should be informed.

PART 6 – USE OF PORTABLE COMPUTER SYSTEMS, USB STICKS OR ANY OTHER REMOVABLE MEDIA

6.1 - Personal, confidential, special-category or safeguarding information must be stored only in school-approved systems and locations. Staff must not copy sensitive school information to personal devices, unapproved USB drives, personal cloud storage or other unapproved media.

6.2 - Where information needs to be accessed off site, staff must use school-approved devices and secure school systems. School information must not be downloaded to or stored on unencrypted or shared personal computers.

6.3 - The school's approved cloud services, including OneDrive where authorised, should be used for secure storage and remote access. Staff must follow sharing permissions carefully and must not move school information into personal cloud accounts.

6.4 - School tablets, laptops and other portable devices must be used in accordance with this policy, the Online Safety Policy and Data Protection Policy. When taken off site, they must remain secure and must be used only for authorised school purposes.

6.5 - School portable devices must be protected by an appropriate passcode, password or other approved authentication and must be locked whenever left unattended.

6.6 - School cameras and other devices containing school information or pupil images must be stored securely and must not be removed from the premises unless authorised for a specific school purpose.

6.7 - School email on portable devices must be accessed through school-approved applications and accounts, including Microsoft 365 Outlook where this is the school's approved arrangement.

PART 7 – USE OF MOBILE PHONES

7.1 - Personal mobile phones, smart watches and other personal devices with messaging, internet or recording functions must be put away when staff begin work with pupils. They should not be carried around or used in classrooms, corridors or playgrounds except where specifically authorised for a genuine emergency, safeguarding, medical or agreed operational reason. Personal use should be limited to designated staff-only areas during authorised breaks.
7.2 - Personal devices must never be used to photograph, film or audio-record pupils, or to store pupil images, personal data, safeguarding information or school records. School-related communication with parents/carers and pupils must use school-approved channels. Devices should also remain put away during prayer, Celebration of the Word, Mass, assemblies, meetings and training unless used for an agreed professional purpose.
7.3 - St Bernadette's is a mobile-phone-free school for pupils during the school day. Where an older pupil needs to carry a phone for the journey to or from school, a parent/carer must complete the school's Mobile Phone Request Form and receive school agreement. Where permission is granted, the phone must be switched off before entering the site and handed directly to Mr Carroll at the start of the day for secure storage in a locked drawer. It will be returned at the end of the school day. In Mr Carroll's absence, a nominated member of SLT will oversee collection, secure storage and return. Reasonable adjustments or exceptional arrangements may be agreed for medical, SEND, safeguarding or other specific needs. See the Behaviour Policy and Online Safety Policy for full procedures.

PART 8 – USE OF DIGITAL IMAGES

8.1 - Images, video and audio of pupils must only be created using school-approved equipment and for a legitimate school purpose. Staff must check and follow current consent and safeguarding arrangements, and images must be stored securely in approved school systems. Personal devices must never be used to photograph, film or audio-record pupils. Images must not be published or shared publicly unless this is authorised through the school's agreed website/social-media arrangements and appropriate permissions are in place.
Official school publication of images, including on the school website or approved school social-media accounts such as Instagram, must follow the Online Safety Policy, consent records and safeguarding requirements. Staff must not publish pupil images through personal accounts.

8.2 – AI-Generated and Manipulated Images

Staff must not upload photographs or videos containing identifiable pupils to public or unauthorised AI tools.
Staff must not create, manipulate or distribute images or videos of pupils in a way that could cause harm, embarrassment, harassment or distress.
Any concerns involving AI-generated or manipulated images of pupils, particularly intimate, sexualised or otherwise harmful images, must be reported immediately to the Designated Safeguarding Lead.

For your own protection it is important that all staff log off after using one of the PCs or laptops to prevent use by another person. On occasion the school will undergo an I.T audit which may reveal that inappropriate material has been viewed. If staff do not log off machines they could be wrongly accused of accessing such material.

PART 9 – USE OF ARTIFICIAL INTELLIGENCE (AI)

9.1 As AI tools become increasingly integrated into education, staff are expected to use them responsibly, ethically and in line with school values, safeguarding requirements, data protection, copyright and professional standards. This section applies to generative AI and other AI-enabled tools used for teaching, administration, assessment, communication or content creation.

9.2 Purposeful and Ethical Use

- AI should only be used to enhance teaching, learning, and administrative efficiency—not to replace professional judgment or human interaction.
- Staff must not use AI to generate or distribute inappropriate, misleading, or discriminatory content.
- Staff will let pupils know when AI has been used to generate images etc, to model ethical use of AI.

9.3 Student Data and Privacy

- Staff must not enter personal, confidential, special-category or safeguarding information about pupils, families or staff into public or unapproved AI systems. Identifiable assessment information, behavioural records, safeguarding records and confidential school documents must only be processed through systems specifically approved by the school with appropriate data-protection safeguards.
- Staff must use only AI tools and services that are approved for the intended school purpose and comply with UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 and school policies.

9.4 Academic Integrity

- Use AI to support, not replace, professional judgement in tasks such as report writing, planning, assessment or communication with parents/carers. AI-assisted drafts must be checked, personalised and verified for accuracy, bias, suitability, safeguarding, confidentiality and copyright before use or sharing. Staff remain professionally responsible for the final content.
- AI-generated teaching materials must be reviewed for accuracy, age-appropriateness, accessibility, bias, safeguarding implications and copyright before use with pupils.

9.5 Safeguarding and Online Safety

- Staff must consider the safeguarding implications of using artificial intelligence tools. AI-generated content may be inaccurate, discriminatory, harmful or inappropriate and may include manipulated images, videos or other content involving pupils or staff.
- Staff must not use AI tools to create, manipulate or distribute harmful, abusive, discriminatory, threatening or sexually explicit content.
- The creation, receipt or discovery of AI-generated or manipulated intimate, sexualised or otherwise harmful images involving pupils must be treated as a safeguarding concern and reported immediately to the Designated Safeguarding Lead or Deputy DSL.
- AI tools accessed through school devices or networks are subject to the school's filtering and monitoring arrangements.

- Staff must only use AI tools in accordance with the school's approved systems, data protection requirements and the terms and age restrictions applicable to those tools.