St. Bernadette's Catholic Primary School
Computing Acceptable Use Policy

Learn to love, love to learn.

Mission Statement

At St. Bernadette's Catholic Primary School you will find us caring, hard-working 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.

Rationale
The policy set out below is that which has been agreed for the acceptable use of the Internet within Birmingham Education Department. All schools should also have an acceptable use policy both for pupils and staff. All of the guidelines have been produced in the light of current legislation including the following Acts.

- **Copyright, Designs and Patent Act (1988)**
- **Human Rights Act (1998)**
- **Regulation of Investigatory Powers Act (2000)**
- **Data Protection Act (1998)**

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 accept 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

St. Bernadette's and the City Council have 3rd party "firewall" software and systems in place to monitor all Internet usage and these will be checked and analysed on a regular basis. Certain sites will be blocked if they are deemed to hold inappropriate or sexually explicit material.

Although St. Bernadette's respects the privacy of every individual throughout the organisation, all external mail (both incoming and outgoing) will be checked for content and attachments to make sure that at all times the security and integrity of St Bernadette's is not impeded. The sender of any message that is intercepted will be notified immediately.

1.5 Disciplinary Process

Action will be taken under St. Bernadette's Disciplinary Policy against any users who are found to breach the policies outlined in these guidelines.
Significant abuse, particularly involving access to pornographic or offensive images constitute gross misconduct leading to summary dismissal.

PART 2 - RESPONSIBILITIES

2.1 Governors and Senior Management Team.

The policies and these guidelines have been approved and adopted by the Governors and Senior Management 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 and the Internet, will be held responsible for complying fully with the St. Bernadette's computer policies and guidelines.

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 BGfL 365 app.

3.2 Confidentiality

Messages sent and received via the Internet are regarded by the Company's Act as having the same legal status as a corporate letter. Any material that is viewed as highly confidential or valuable to the school should not be emailed externally.

Emails containing personal/ sensitive information should be sent encrypted to the recipient.

A disclaimer document will be attached to all emails. In no instance should the disclaimer be tampered with, although if necessary the signature can be altered.

It should be remembered that the Internet does not guarantee delivery or confidentiality. When responding to parents queries, staff should respond from their year band email account.

For security and privacy reasons, use the Blind Carbon Copy (Bcc) feature when sending an email message to a large number of people or when contacting outside agencies. This conceals the person entered in the Bcc field from the other recipients.

It should be noted **that there are systems in place that can monitor, review and record all email usage, and these will be used**. Analysis of this information may be issued to the Senior Management team and the Governors if thought appropriate. No user should have any expectation of privacy as to his or her email.

3.3 Etiquette
At all times users should use appropriate etiquette when writing emails. Care should be taken when addressing emails, particularly when using address groups, in order to send them to only those recipients who will have an interest. 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
Email is an effective way of communicating confidential information. This is only the case, however, if passwords are secure. To maintain security it is good practice for users to change their passwords regularly.

Email should not be left running unattended in any circumstances where this may lead to unauthorised access. The system should be closed and re-opened on return. In no instances should a user login using a colleague's password unless

permission has been given.

3.9 Housekeeping

Good housekeeping practices should be adopted so that files are deleted regularly or, if necessary, archived to a separate file. Mailbox sizes will be reviewed regularly and warnings will be issued to users with files of 100MB or larger.

File attachments, incoming or outgoing through the firewall, are limited to 15MB but good practice is that file attachments should only be sent to a minimum of recipients and not all if they are large files.

PART 4 - INTERNET GUIDELINES

4.1 Rules for business use

All users will be provided with access to the Internet through the Birmingham Grid for Learning.

Users should not download any material that is not directly related to their job responsibility. This especially relates to screensavers, images, videos games etc. The ICT co-ordinator should be notified before any software is downloaded for business use: all downloaded software needs to be properly licensed and registered. Any such software automatically becomes the property of the school. **There are systems in place to monitor all Internet usage including any software downloads.**

4.2 Personal use

Employees are permitted to access the Internet for personal use on a limited basis as long as this does not interfere with their job responsibilities. This should be in own time, i.e. before or after school, or with the permission of the Headteacher.
It should be noted that there are systems in place that can monitor and record all Internet usage, and these will be used. No user should have any expectation of privacy as to his or her Internet usage. Analysis of this information may be issued to the Senior Management team or Governors if thought appropriate.

4.3 Respecting copyright

Employees with Internet access must comply with the copyright laws of all countries relevant to Education Services. Users must not intentionally download any material that holds a copyright notice. This also relates to downloading and copying unlicensed software.

4.4 Security

Systems are in place to protect the school's information systems. However, users must also be aware of the potential risks associated with accessing the Internet. Employees are reminded that newsgroups are public forums where it may be inappropriate to reveal confidential information.

Also, see section 4.2 above.

Users are also reminded that unauthorised usage of a computer could include accessing email or the Internet via a computer other than your own even if doing so under your own user identification, and could contravene City Council ICT Security Policy and even Computer Misuse legislation.

4.5 Virus protection

Although virus protection software is installed on all networked computers, users should be aware of the potential hazards associated with computer viruses. Any files that are downloaded will be scanned for viruses before being accessed. If you have any concerns about viruses on the Internet or think you may have accessed material that contains a virus please contact ICT co-ordinator or school technician.

4.6 Inappropriate websites

Under no circumstances should a user access a site that contains sexually explicit or offensive material. **If you find yourself connected to such a site inadvertently, you should disconnect from that site immediately, and notify the ICT co-ordinator who will log the incident.**

Because individuals may consider a wide variety of material offensive, users should not store, view, print or redistribute any material that is not directly related to the user's role or the school's activities.

PART 5 – SOCIAL NETWORKING SITES

The school recognises that many staff will actively use Facebook, Twitter and other such social networking sites, blogging and messaging services. The following guidelines form the school policy for use of such sites.

General guidelines for use of social networking sites:

- Staff must not have any contact with current pupils at St Bernadette's through such sites.
- Staff profile security should be set to maximum levels.
- Staff must ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friend's only' level of visibility.
- Staff should be aware that more distinctive surnames will be easy to track down using the search tool on such social networking sites, and that these services will display a profile picture and some personal information, regardless of security settings.
- Staff should not reveal confidential or sensitive information, with regards to other staff or pupils.
- Unless authorised to do so, staff must not post content on websites that may appear as if they are speaking for the school.
- Staff should not post any material online that can be clearly linked to the school or that may damage the school's reputation.

- Staff should avoid posting any material which could clearly identify themselves, another member of staff, or a pupil. This will avoid the risk of the information potentially being used to embarrass, harass, or defame the subject.

Staff Profiles

5.1 Statuses/comments

- Staff should not post comments/statuses which bring the school or pupils into disrepute.
- Staff should not name pupils in such comments/statuses.
- Staff should use discretion when naming other staff in comments/statuses.

5.2 Photos/videos

- Staff must use their discretion when deciding suitable, personal photos to post.
- Staff must seek permission of other staff if they wish to post photographs in which these staff appear.
- Photo albums should be set to maximum security.

Contact with pupils

5.3 Friends

- Staff must not add any pupils to their 'friends list'.
- If a request is made by a child, staff should decline and report the incident to the ICT Coordinator, who will speak to the child in question and report the incident to parents/guardians.
- Staff should use their discretion when accepting parents/parent helpers as friends.
- Staff should use discretion in terms of accepting past pupils, who are not minors. In the case of minors staff should reject the request.

5.4 Messages

- Staff must not message any pupils for any reason over social networking sites, even for school-related purposes.
- If at any time, a member of staff receives a message from a pupil, they must not reply. They should notify the ICT Coordinator, who will speak to the child in question and report the incident to parents/guardians.

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

6.1 - All sensitive data, such as children's details and reports, should be stored on an encrypted storage device or a school password-protected laptop. Other data, such as lesson plans and resources, may be stored on unencrypted devices. Each memory stick is assigned to one member of staff and logged.

6.2 - If data is taken off-site it is not to be loaded onto unencrypted computers at home.

6.3 – Sensitive data can also be uploaded to the school's encrypted file hosting service (OneDrive). Files are not be downloaded onto unencrypted computers. If off-site, staff should edit and save the data on the cloud sharing service.

6.4 – Tablet devices such as iPads must be used in accordance with earlier acceptable use guidelines (see part 4). Such devices, when used off the school premises, must only be used for directed activities such as for the purpose of assessment.

6.5 – When not in use, tablet devices must be passcode protected at all times.

6.5 – Digital cameras and any other unprotected devices must be stored safely at all times and not removed from the premises.

6.5 – Emails should be accessed using the BGfL 365 app only when using portable devices.

PART 7 – USE OF MOBILE PHONES

7.1 - Staff should NOT use their personal phones for school business or for taking photographs of children. Unless, in exceptional circumstances, an emergency telephone call needs to be made.
7.2 - Mobile phones should not be used when teaching, unless in an emergency.
7.3 - Pupils should NOT bring mobile phones to school. (See Online Safety policy)

PART 8 – USE OF DIGITAL IMAGES

8. 1 - Any photos or videos taken by teachers, other adults (including parents), and the children themselves during ANY school activity (including trips / camp) should not be put on public display or published anywhere on the internet (including social networking sites such as Facebook).
The above excludes the publication of photos on the school website/Twitter (See Online Safety policy for guidelines) as well as use by school for educational/display uses.

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.

Aimee Hulse
Computing Co-ordinator
Updated June 2022