ICT ACCEPTABLE USE POLICY FOR LEARNERS

Achieve, Believe, Care

St Bernadette's Catholic Primary School

ICT Acceptable Use Policy For Learners

The following guidelines are for use for any computer on the network:

General Conduct and Use

- Computers may be adjusted for comfort and ease of use but must be adjusted back after use for the next user.
- No food or drink may be consumed around a computer or in any computer suite.
- Damage to computer equipment or furniture will not be tolerated. It you see anyone causing any damage you should report it to a member of staff without delay.
- Chairs should be placed tidily in the rooms before departure.

Use of the Network

- Do not disclose your login username and password to anyone.
- All users must use their own unique username and password. Any attempt or use of anybody else's username is strictly forbidden and means that, once discovered, the person committing the identity theft and, where applicable, the person who gave out his/her user name/password will be severely punished in line with school policy.
- Before leaving a computer, users must log off the network and check that the logging off procedure is complete.
- Only software provided by the network may be run on the computers. Users are not permitted to import or download applications or games.
- You must not use any removable devices (USB Pens) if you are unsure of their content or origin.
- You must not use your area to store videos and/or music. All files of banned types will be deleted nightly.
- Viruses are strictly banned from the network and any user who brings in or downloads a virus will be logged and disciplinary action will be taken.

Mobile Device Policy (including Laptops, PDAs & Netbooks)

The following guidelines are for use of any mobile device:

- Access to the school's wireless network must be approved by a member of IT Support.
- Under no circumstances must a computer, printer or other device be detached to allow a PDA or laptop access to charge
- Laptops from outside the school must have up to date, school approved anti---virus protection installed before being connected to the network

Internet Safety Policy

The following rules are guidelines for the safety of users when on the internet:

- Never give out personal information such as an address, telephone number, mobile number over the internet without being sure that the receiver is from a reputable source. If you are unsure, ask an adult.
- Always alert a member of staff or an adult if you view content that makes you feel uncomfortable.
- Never send a picture of yourself and/or friends to any receiver that is not from a reputable source. If

you are unsure, ask an adult.

- Always alert a member of staff or an adult if you receive any messages that make you feel uncomfortable.
- Never arrange to meet anybody from the internet. Tell your parents if someone asks to meet you.

Acceptable Internet and Email Policy

- The Internet and e---mail facilities are provided to support learning and teaching at St. Bernadette's. They should be used with care and responsibility and with respect for other users.
- **DO NOT** send electronic messages which are impolite, indecent, abusive, discriminating, racist, or in any way intended to make the recipient feel uncomfortable. Your actions could be perceived as bullying or intimidation.
- **DO NOT** access any sites which may contain inappropriate material or facilities, as described below:
    - Proxy Sites
    - Dating
    - Hacking
    - Pornography
    - Malicious Words or Images
    - Music Download
    - Inappropriate Games
    - Gambling
- **DO NOT** send pictures of other pupils/students or any malicious, violent or pornographic images/videos, through any form of electronic communication, including mobile phones. If you are involved in these activities **you are breaking the law**. The consequences of these actions will be a ban from the internet, your parents being informed and the possibility of further disciplinary action or police involvement.
- **DO NOT** upload or download unauthorised software and attempt to *run* it on a networked computer: in particular hacking, encryption and virus software.
- **DO NOT** use the computer network to gain unauthorised access to any other computer network.
- **DO NOT** attempt to spread viruses.
- **DO NOT** engage in activities that are prohibited under UK Law. Thus the transmission of material subject to copyright or protected by trade secret is forbidden.
- **NEVER** open attachments of files if you are unsure of their origin.
- **YOU** must only access those services you have been given permission to use.
- **DO NOT** download, use or upload any material from the Internet, unless you have the owner's permission.

- **UNDER NO** circumstances, should you view, download, store, distribute or upload any material that is likely to be unsuitable for children or school. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any use which may be likely to cause offence. If you are not sure about this, or come across any such materials, you must inform the Digital Resources Manager or Learning Technologies Technician.
- **ALWAYS** respect the privacy of files of other Users.
- **AVOID** any acts of vandalism on the network. This includes, but is not limited to, uploading or creating computer viruses and mischievously deleting or altering data from its place of storage.

Acceptable use of the Virtual Learning Environment

- Users are responsible for their own good behaviour and should consider their messages and communications as being similar in all respects to any conversation in a classroom or a school corridor. General rules of good and respectful behaviour apply.

In addition, the following acts are prohibited and will not be tolerated:

- Sending or displaying any abusive, sexist, racist or otherwise offensive material.
- Using obscene language.
- Accessing, or attempting to access, any inappropriate or offensive material; uploading, posting, e---mailing or otherwise transmitting any content that is unlawful, harmful, threatening, abusive, harassing, defamatory, vulgar, obscene, libellous, invasive of another's privacy, hateful, or racially, ethnically or otherwise objectionable.
- Violating copyright laws.
- Attempting to harm minors (people who are under the age of 16) in any way.
- Impersonating of any person or entity, or falsely stating or otherwise misrepresenting an affiliation with a person or entity.
- Forging headers or otherwise manipulating identifiers in order to disguise the origin of any content transmitted through any internet service.
- Uploading, posting, messaging or otherwise transmitting any content that is without right to transmit under any law or under contractual or fiduciary relationships (such as inside information, proprietary and confidential information learned or disclosed as part of employment relationships or under nondisclosure agreements).
- Uploading, posting, messaging or otherwise transmitting any content that infringes any patent, trademark, trade secret, copyright or other proprietary rights ("Rights") of any party.
- Uploading, posting, messaging or otherwise transmitting any unsolicited or unauthorised advertising, promotional materials, "junk mail", "spam", "chain letters", "pyramid schemes", or any other form of solicitation.
- Uploading, posting, messaging or otherwise transmitting any material that contains software viruses or any other computer code, files or programmes designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment.
- "Stalking" or otherwise harassing any user or member of staff.
- Collection or storage of personal data about other users.
- Contacting members of staff through any Internet facility other than what is provided by the school, e.g. Social Networking
- Upload any images or videos to YouTube without prior consent of all parties' involved (parental consent needed for all people under the age of 18).