Computing and E-Safety Policy

Contents Page

1 Introduction

Information and Communication Technology (ICT) in the 21st Century is recognised as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality
- Gaming, especially online
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements, usually 13 years.

At St Bernadette's, we understand the responsibility to educate our pupils on E-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

2 Roles and Responsibilities

As E-Safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The E-Safety co-ordinator is a member of the senior leadership team and is a designated leader of Child Protection within the school.

This policy, supported by the school's Acceptable Use agreements for staff and pupils, is to protect the interests and safety of the whole school community. It is linked to the following school policies and procedures: Child Protection, Health and Safety, Behaviour (including anti-bullying), British Values, Staff Code of Conduct.

3 E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We ensure that E-Safety guidance is given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote E-Safety.

- The school provides opportunities within a range of curriculum areas to teach about E-Safety.

- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as is part of the E-Safety curriculum.

- Pupils are taught about the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

- Pupils are taught about copyright, respecting other people's information and protecting their own personal information, safe use of images and other important areas through discussion, modeling and appropriate activities.

- Pupils are taught about the impact of Cyberbullying and are taught how to seek help if they are affected by any form of online bullying.

- The school uses ThinkUKnow and Childnet resources to teach pupils how to keep safe online and steps to take if they are made to feel uncomfortable or experience examples of grooming which could lead to Child Sexual Exploitation (CSE) or other criminal behaviour

- Pupils are taught where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cybermentors, Childline or the CEOP report abuse button.

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

4 Pupils with Additional Needs

- The school recognises that Some groups of children are potentially more vulnerable and more at risk than others when using ICT. These can include children with emotional or behavioural difficulties, learning difficulties, and other complex needs, as well as those whose English is an additional language, and looked after children. Pupils with additional needs may be more vulnerable to the risk of online grooming via the internet and therefore staff monitor these pupils' use of the internet closely and liaise with parents where appropriate. This highlighted within staff training.

- The school endeavors to create a consistent message with parents for all pupils and this in turn should aid the establishment and future development of our E-Safety rules. However, staff are aware that some pupils may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of E-Safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of E-Safety. Internet activities are planned and well managed for these children and young people.

5 E-Mail

The use of e-mail within school is an essential means of communication. In the context of school, e-mail should not be considered private. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette; 'netiquette' and how to send and receive emails by the end of Year 2.

- The school gives all staff their own e-mail account to use for all school business as a work based tool This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school related business.

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

- All e-mails should be written and proof-read carefully before sending, in the same way as a letter written on school headed paper.

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

- E-mails created or received as part of staff's school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage their e-mail accounts as follows:

- -Delete all e-mails of short-term value

- -Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- Where relevant to the computing curriculum, pupils have access to class email addresses, with password controlled by the class teacher and changed following each session.

- The forwarding of chain letters is not permitted in school.

- All pupil e-mail users are expected to adhere to the generally accepted rules of netiquette particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments. Emails must not be used by any member of the school community to send or receive indecent or offensive images, videos or any written material of this kind. In addition, emails must not be used by any member of the school community to cause intentional harm, upset, directly or indirectly to others.

- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail whether directed at themselves or others and before it is deleted.

- Staff must inform the E-Safety co-coordinator or Headteacher if they receive an offensive e-mail whether it is directed at themselves or others and before it is deleted.

- Pupils are introduced to e-mail as part of the ICT curriculum.

Sending E-Mails

- Staff must use their own school e-mail account so that they are clearly identified as the originator of a message.

- Staff must keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

- Staff must not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

- School e-mail is not to be used for personal advertising.

Receiving E-Mails

- Staff must check e-mail regularly.

- Staff should activate the ‘out-of-office’ notification when away for extended periods.

- Staff must never open attachments from an untrusted source; Consult the ICT leader or technician first if in doubt.

- Staff must not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

- The automatic forwarding and deletion of e-mails is not allowed.

6 E-Safety Support for Staff

- Our staff receive regular and appropriate information and training on E-Safety and how they can promote the ‘Stay Safe’ online messages. This is usually through the usual scheduled programme of staff meetings.

- New staff receive information on the school's acceptable use policy as part of their induction.

- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of E Safety and know what to do in the event of misuse of technology by any member of the school community.

- All staff are encouraged to incorporate E-Safety activities and awareness within their curriculum areas.

7 The Internet

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of the internet is logged and the logs are randomly but regularly monitored by our broadband provider, *Updata*. Whenever any inappropriate use is detected it will be followed up.

- The school provides pupils with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.

- Staff will preview any recommended sites before use.

- Raw image searches are discouraged when working with pupils.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

- All users must observe copyright of materials from electronic resources.

- On-line gambling or gaming is not allowed.

- All staff, volunteers and governors must comply with the ICT Acceptable Use Policy regarding the posting of any information or images relating to the school.

- School internet access is controlled through the LA recommended broadband supplier, *Updata*, who provide a filtering service.

- St Bernadette's is aware of its responsibility when monitoring staff communication under current legislation.

- Staff and pupils are aware that school based email and internet activity can be monitored and explored further if required.

- The school does not allow pupils access to internet logs.

- The school uses management control tools for controlling and monitoring workstations

- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the e-safety coordinator or teacher as appropriate.

- It is the responsibility of the school, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.

- Pupils are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT leader.

- If there are any issues related to viruses or anti-virus software, the ICT leader should be informed immediately.

- The school does not allow any access to social networking sites.

- Many extremist groups such as far right groups, animal rights activists and Islamic fundamentalists who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences. Staff are provided with PREVENT and/or Channel training to support them in identification of such young people who may be targeted by or exposed to harmful influences from violent extremists via the internet. Adequate filtering is in place to prevent pupils and staff from accessing websites advocating violent extremism. Referrals are made to MASH/police where there is any evidence of pupils' exposure to extremist narrative and/or if there is evidence that their parents are involved in advocating extremist violence.

We believe that it is essential for parents/carers to be fully involved with promoting E-Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss E-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

8. Youth Produced Sexual Imagery (Sexting)

In cases of Youth Produced Sexual Imagery (Sexting), we follow guidance given to schools and colleges by the UK Council for Child Internet Safety (UKCCIS) published in August 2016: 'Sexting in schools and colleges, responding to incidents, and safeguarding young people'.A SRE policy and curriculum has been adopted by Governors to help children to understand the risk and keep themselves safe.

When an incident involving youth produced sexual imagery comes our attention,

- The incident will be referred to the DSL as soon as possible

- The DSL will hold an initial review meeting with appropriate school staff, then with the young people involved (if appropriate)

- Parents will be informed at an early stage and involved in the process unless there is good reason to believe that involving parents would put the young person at risk of harm

- At any point in the process if there is a concern a young person has been harmed or is at risk of harm a referral should be made to children's social care and/or the police immediately.

9 Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness. With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment

- Staff and visitors are not permitted to use **personal** digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on educational visits. Appropriate images can be taken using school cameras; these should be transferred as soon as possible to the school's network and deleted from the individual device.

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from the Headteacher.

- Staff must have permission from the Headteacher before any image can be uploaded for publication.

- Permission to use images of all staff who work at the school is sought when needed.

- Where an outside company or individual is commissioned by the school to take images, there must be appropriate DBS clearance and the school should satisfy itself that appropriate arrangements are in place to ensure images are not stored or distributed outside of the school.

10 Publishing Pupil's Images and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site.

- in the school prospectus and other printed publications that the school may produce for promotional purposes.

- recorded/ transmitted on a video or webcam.

- in display material that may be used in the school's communal areas.

- in display material that may be used in external areas, i.e. exhibition promoting the school.

- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. However, it is the practice of the school to ask parents to re-sign this annually at the beginning of each new school year and parents or carers may withdraw permission, in writing, at any time.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published. Before posting a child's work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

11 Storage of Images

- Images/ films of children are stored on the school's network.

- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network or other online school resource.

12 Web Cams and CCTV

- We do not use publicly accessible webcams in school.
- Webcams in school are only ever used for specific learning purposes.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document). Staff must ensure web cams are switched off when not in use.

13 Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences
- All pupils are supervised by a member of staff when video conferencing.
- The school keeps a record of video conferences, including date, time and participants.
- Approval from the Headteacher is sought prior to all video conferences within school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

14 Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/carer using their personal device.
- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate messages, images (including pseudo images), videos or sounds between any members of the school community is not allowed.
- The creation of inappropriate messages, images (including pseudo images), videos or sounds by any member of the school community is not allowed.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

15 Parental Involvement

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website).See appendix 5

- The school disseminates information to parents relating to E Safety where appropriate in the form of:

    - Information and celebration evenings
    - Practical training sessions
    - Newsletter items

16 Security

The school gives relevant staff access to its Management Information System, with a unique username and password

- It is the responsibility of everyone to keep passwords secure; passwords are not to be shared with others.

- Staff are aware of their responsibility when accessing school data

- Staff have been issued with the relevant guidance documents and the Policy for Acceptable Use

- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data

- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight

- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

- All ICT equipment is security marked as soon as possible after it is received. The School Business Manager maintains a register of all ICT equipment and other portable assets which is kept online with *Parago*, a secure website for asset tracking.

- As a user of the school ICT equipment, you are responsible for your activity.

- ICT equipment issued to staff is logged and serial numbers are recorded as part of the school's inventory.

- It is imperative that staff save data on a frequent basis to the school's network. Staff are responsible for the backup and restoration of any of your data that is not held on the school's network.

- Personal or sensitive data should not be stored on the local drives of desktop PC, laptop, USB memory stick or other portable devices. If it is necessary to do so the local drive must be encrypted.

- It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.

- Privately owned ICT equipment should not be used on a school network.

- On termination of employment, resignation or transfer, staff must return all ICT equipment to the school. Staff must also provide details of all their system logons so that they can be disabled.

- All activities carried out on school systems and hardware will be monitored in accordance with the general policy.

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

- Portable equipment must be transported in its protective bag.

- Anyone expecting a confidential or sensitive fax should notify the sender before it is sent.

- Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult for the school to use technology to benefit learners. Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties

Server Security

- School servers are kept in a locked and secure environment and there are limited access rights to these which are password protected.

- Existing servers should have security software installed appropriate to the machine's specification and the school uses a remote back up service for the Admin Drive and data is backed up daily. The Curriculum Drive is backed up onsite every three days.

Using Removable Media

- Always consider if an alternative solution already exists.
- Only use recommended removable media.
- Store all removable media securely.
- Removable media must be disposed of securely by our ICT support team.

Monitoring

- Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices.

- Internet activity is logged by the school's internet provider and in addition the school's technicians regularly monitor the web sites which are accessed on school equipment.

17 Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school computer hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

18 Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's E-Safety Co-ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported. See Appendices 3 and 4 for reporting template and procedures.

An incident log is used to monitor what is happening and identify trends or specific concerns. The log is kept in the Head Teacher's office.

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the E-Safety co-ordinator

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the E-Safety co-ordinator, depending on the seriousness of the offence; investigation by the Headteacher/ LA, possibly leading to disciplinary action, dismissal and involvement of police for very serious offences.

19 Protecting Personal, Sensitive, Confidential and Classified Information

Staff will ensure:

- They lock their screen before moving away from their computer during the normal working day to prevent unauthorised access

- Personal, sensitive, confidential or classified information is not disclosed to any unauthorised person

- The security of any personal, sensitive, confidential and classified information contained in documents which are faxed, copied, scanned or printed.

- They only download personal data from systems if expressly authorised to do so by the Headteacher.

- They keep their screen display out of direct view of any third parties when accessing personal, sensitive, confidential or classified information.

- Hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

- They protect school information and data at all times, including any printed material.

20 Viruses

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

- Never interfere with any anti-virus software installed on school computer equipment that you use.

- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

- If you suspect there may be a virus on any school ICT equipment, disconnect from the network, stop using the equipment, shut down, and contact the ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

21 Disposal of ICT Equipment

- All redundant ICT equipment will be disposed of through an authorised agency recommended by the LA. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. Any redundant ICT equipment being considered for sale / gift will have been subject to a recent electrical safety check and hold a valid PAT certificate and if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.

Disposal of any ICT equipment will conform to current legislation and will confirm with the governors' policy on the disposal of equipment.

22 Zombie Accounts

Zombie accounts refer to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

- Technical staff will ensure that all user accounts are disabled once the member of the school has left the school.

Appendix 1

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 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'm 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 if I deliberately misuse it.

@ I understand that information on the internet may not always be reliable and sources may need checking.

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: _________

St Bernadette’s Catholic Primary School
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.

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. Activities such as buying or selling goods are inappropriate.
- Always check files brought in on removable media (such as floppy disks, CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- Always check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else’s logon name or password.
- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- 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 your work at risk.
- Computer storage areas and floppy disks will be treated like school lockers. ICT staff may review your files and communications to ensure that you are using the system responsibly.

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.
- ‘Chat’ activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons ‘chat’ rooms should not be used.

Email

The use of electronic communication and information retrieval is no more than the addition of another medium. The same behavioural and professional standards are expected of employees as are the case with traditional written communications, the telephone and face to face meetings.

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Remember you are a representative of the school and that you are using a non-private network.
- 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.
- Any communication with parents should be conducted via your school email account and not personal accounts.
- 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 and the school’s network.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

Social Networking sites

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

- Social media should not be accessed on the school’s premises
- Do not speak for the school unless you have express permission to do so, this covers all comments relating to the school
- Do not register your place of work on any social media
- Protect yourself from identity theft
- 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 until they have left us by four years 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

E-Safety Incident Report

Incident No:

Date of Incident:	Location of Incident:

Name of person who discovered / identified incident:

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

Comments / Notes

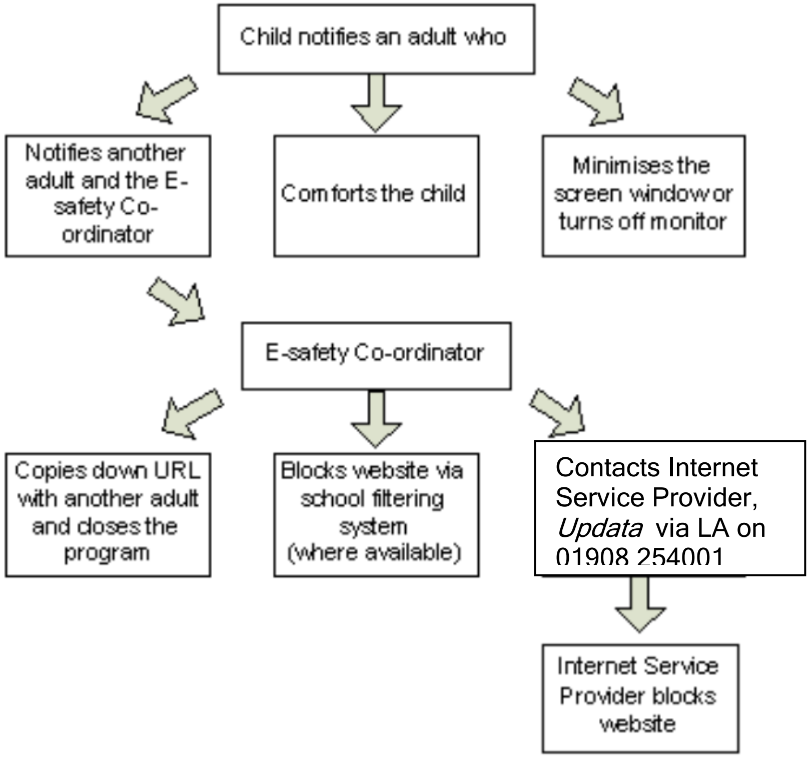
Date form sent to E-safety Co-ordinator	Signature

Appendix 4

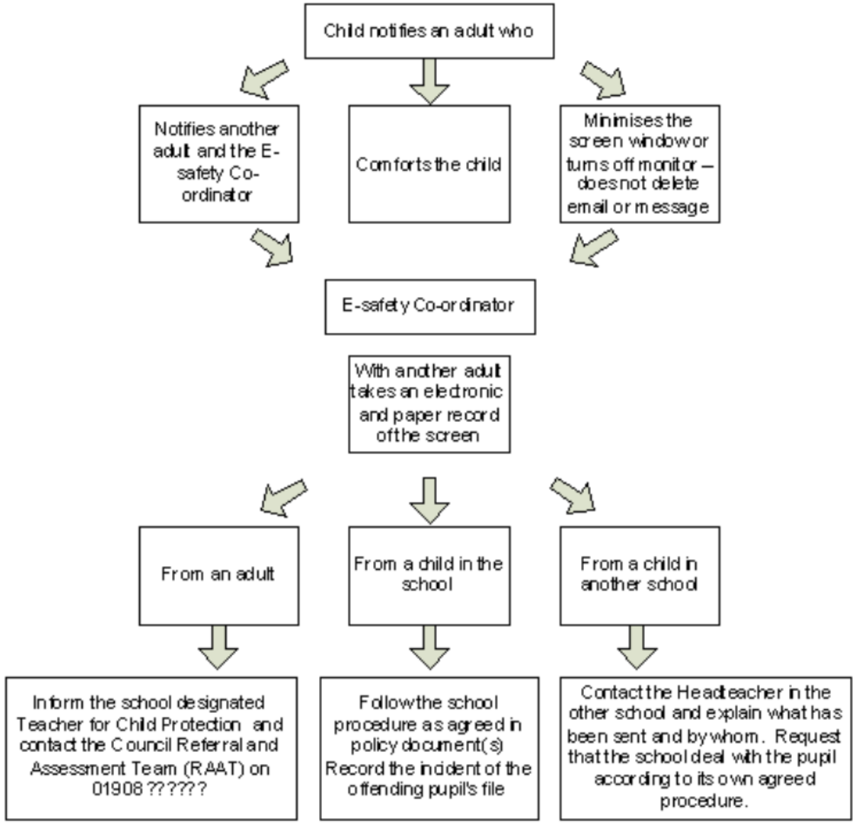
St Bernadette's Catholic Primary School

E-Safety Reporting Incidents Procedures

E-safety Incident – View of Inappropriate Material


Child notifies an adult who
Notifies another adult and the E-safety Co-ordinator
Comforts the child
Minimises the screen window or turns off monitor
E-safety Co-ordinator
Copies down URL with another adult and closes the program
Blocks website via school filtering system (where available)
Contacts Internet Service Provider, *Updata* via LA on 01908 254001
Internet Service Provider blocks website

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


Child notifies an adult who
Notifies another adult and the E-safety Co-ordinator
Comforts the child
Minimises the screen window or turns off monitor – does not delete email or message
E-safety Co-ordinator
With another adult takes an electronic and paper record of the screen
From an adult
From a child in the school
From a child in another school
Inform the school designated Teacher for Child Protection and contact the Council Referral and Assessment Team (RAAT) on 01908 ??????
Follow the school procedure as agreed in policy document(s) Record the incident of the offending pupil's file
Contact the Headteacher in the other school and explain what has been sent and by whom. Request that the school deal with the pupil according to its own agreed procedure.

Appendix 5

Parental Permissions

Dear Parents and Carers,

The following paragraphs outline activities for which we need to obtain your specific approval. The form will stand for the time your child is at St Bernadette's or until legislation requires us to amend the details, however, it is the practice of the school to ask you to re-sign this annually at the beginning of each school year. Parents and carers may withdraw permission, in writing, at any time. Please read each section on both pages carefully, delete and sign as appropriate, and return the form to school – thank you.

Yours faithfully

M. Clewlow.

Mrs Clewlow

CHILD'S NAME ………………………………………………………………. Date of birth ………/……../………

THE LIBRARY

In the library our books are barcoded and information about each book is held on the computer. We would like to ask you to ensure that all books taken home are treated with care and returned promptly. You will appreciate that books are expensive and if they are lost you will be responsible for the cost of any necessary replacement.

I give/I do not give my permission for my child to borrow books from the library.

Signed ……………………………………………………………(Parent/Carer)

PHOTOGRAPHS/IMAGES/PUPILS' WORK

We like to take photographs of our pupils which may be used for displays, as records of work/events, for publication in the diocesan/local press or on the school website, prospectus or other printed publications that the school may produce for informative or promotional purposes. Names of children will not be published. As part of the ICT curriculum, we may also record or transmit images of your child via video or webcam, using video conferencing. We also use videos for staff training and development (Iris Connect) We may also wish to publish examples of pupils' work.

I give/I do not give my permission for my child's photograph to be taken and images or examples of his/her work to be used as detailed above.

Signed ……………………………………………………………(Parent/Carer)

THE INTERNET

Internet access is part of the statutory curriculum. Pupils will be given clear objectives for Internet use and staff will select sites which will support the planned learning outcomes. Some of the material used in school will be on a cache system which means the children will not be live on the Internet. However, there may be occasions when direct access is required and it is for these occasions that we need your permission. Our Internet access provider operates a filtering system that restricts access to known inappropriate materials. Every endeavour will be made to ensure suitable restrictions are effective. However, neither the school nor Milton Keynes Council will be held responsible for the nature or content of material accessed through the Internet. Parents will be informed if any inappropriate material is viewed.

I give/I do not give my permission for my child to access the Internet.

Signed ……………………………………………………………(Parent/Carer)

SCHOOL VISITS AND ACTIVITIES

Children will take part in activities offsite and sometimes outside school hours. These activities are planned to support the curriculum and/or to provide additional opportunities, which we hope your child will find helpful and enjoyable, eg visiting the locality, another school, swimming lessons. Such visits and activities will be properly organised and all reasonable precautions will be taken for the safety and wellbeing of your child. Nevertheless, it is possible that your child may be exposed to additional hazards, e.g. accidents in the course of travel or sporting activities, when urgent medical treatment might be needed in circumstances where it is not possible to contact the parent/carer. In this situation, we hope you would be willing to agree that the teacher in charge of any party may give the necessary consent on your behalf. Please note that for longer trips parents will receive more detailed information and you will need to give specific written permission for these visits, separate from this form.

I give/I do not give my permission to participate in school visits/activities and for any urgent medical treatment to be administered.

Signed ……………………………………………………………(Parent/Carer) Date ………/………/………

Appendix 6

Parental Letter Example - Social Media use

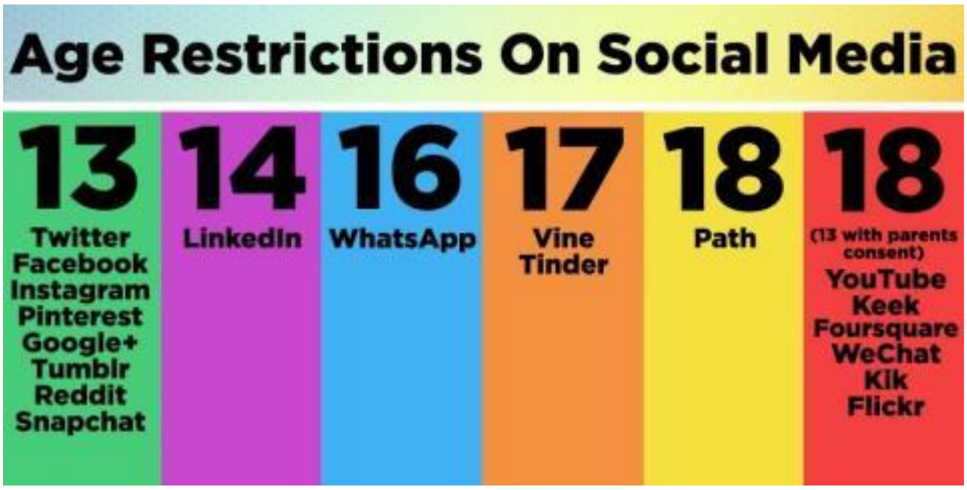
16th November 2016

Dear Parents/Carers,

It has come to my attention that pupils within Key Stage 2 are accessing a range of social media which legally they should not be using.

I have alo been made aware that some of the interactions between pupils whilst using social media have been offensive and inappropriate.

I would like to draw your attention to the age restrictions regarding a range of popular social media.



Age Restrictions On Social Media

13	14	16	17	18	18
Twitter Facebook Instagram Pinterest Google+ Tumblr Reddit Snapchat	LinkedIn	WhatsApp	Vine Tinder	Path	(13 with parents consent) YouTube Keek Foursquare WeChat Kik Flickr

I urge you to monitor your child's use of social media and respect the above age restrictions to ensure that your child is keeping themselves safe online.

Yours faithfully,

M. Clewlow.

Mrs Clewlow
(Headteacher)