ST JOHN THE BAPTIST C OF E PRIMARY SCHOOL

E- SAFETY POLICY

Reviewed:	February 2020
Next Review:	February 2022
Person Responsible:	John Cumming

e-SAFETY POLICY

1. Aims and Objectives

1.1 ICT in the 21st Century is seen 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 provide our young people with the skills to access life-long learning and employment.
Information and Communications Technology 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

1.2 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.

1.3 At **St John the Baptist C of E Primary School** 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.

1.4 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.

1.5 **Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.**

1.6 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, tablets, webcams, whiteboards, voting systems, digital video equipment; and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, smart phones and portable media players).

2. Monitoring

2.1 Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge. Any ICT authorised staff member will be happy to comply with this request.

2.2 ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

2.3 ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

2.4 All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

3. Breaches

3.1 **A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT 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.
The ICO's new powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessments to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;

- Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

4. Incident Reporting

4.1 **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 ICT Co-ordinator**. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to a member of the Senior Leadership Team.

5. Computer Viruses

5.1 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.

5.2 Staff will ensure that they never interfere with any anti-virus software installed on school ICT equipment that they use.

5.3 If a staff machine is not routinely connected to the school network, they must make provision for regular virus updates through the ICT coordinator.

5.4 If staff suspect there may be a virus on any school ICT equipment, they must stop using the equipment and contact the ICT coordinator or technician immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

6. Email

6.1 The use of e-mail within most schools is an essential means of communication for both staff and pupils. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or pupil based, within school or international. We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette. Pupils are taught how to safely and effectively send and receive emails as part of the Computing curriculum.

7. Managing Email

7.1 'Exa' 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.

7.2 **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 business.

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

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

7.5 Staff sending e-mails to external organisations, parents or pupils are advised to cc. the Headteacher or a member of the Senior Leadership Team.

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

7.7 E-mails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your e-mail account 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

7.8 All children have their own gmail email account. The ICT coordinators, office staff and ICT Technician have access to passwords and email addresses.

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

7.10 All pupil e-mail users are expected to adhere to the generally accepted rules of etiquette, 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.

7.11 Pupils must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

7.12 Staff must inform ICT coordinators if they receive an offensive e-mail.

7.13 Pupils are introduced to e-mail and safe Internet use as part of the Computing Scheme of Work, E-safety scheme of work and are reminded about this learning each time they access the internet in school.

7.14 However you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

8. Sending Email

8.1 Use your own school e-mail account so that you are clearly identified as the originator of a message.

8.2 Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

8.3 Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

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

9. Receiving Email

9.1 Staff have been advised by the head teacher to check their e-mail daily.

9.2 Activate an 'out-of-office' notification when away for extended periods.

9.3 Never open attachments from an untrustworthy source; consult the ICT coordinators.

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

10. Security

10.1 I**t is the responsibility of everyone to keep passwords secure.**

10.2 Staff are aware of their responsibility when accessing school data.

10.3 Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.

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

10.5 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.

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

10.7 **Staff have all been issued with password protected memory sticks which they must use to store any sensitive, confidential or classified data including information on pupil progress.**

10.8 **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.**

11. Disposal of redundant ICT equipment

11.1 All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

11.2 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. We will only use authorised companies who will supply a written guarantee that this will happen.

12. e-Safety roles and responsibilties

12.1 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.

12.2 **The named e-Safety co-ordinator in this school is John Cumming. He has been designated this role as part of Computing Leader responsibilities.** All members of the school community have been made aware of who holds this post.

12.3 Senior Management and Governors are updated by the Head/ e-Safety co-ordinator and all Governors have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

12.4 This policy, supported by the school's acceptable use agreements for staff, governors, visitors and pupils, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/pupil discipline (including the anti-bullying) policy

13. Equal opportunities – Pupils with additional needs

13.1 St John the Baptist C of E Primary School endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' 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.

13.2 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 pupils.

14. e-Safety in the curriculum

14.1 ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be 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.

14.2 The school has e-Safety planning for teaching internet skills in computing lessons.

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

14.4 Educating pupils about online risks that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.

14.5 Pupils are aware of 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.

14.6 Pupils are taught about copyright, respecting other people's information and safe use of images through discussion, modelling and appropriate activities.

14.7 Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of 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.

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

15. e-Safety skills development for staff

15.1 Our staff receive regular information and training on e-Safety issues.

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

15.3 **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.**

15.4 All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas, where relevant.

16. Managing the school's e-Safety messages

16.1 We endeavour to embed e-Safety messages across the curriculum whenever the Internet and/or related technologies are used.

16.2 The e-Safety policy will be introduced to the pupils at the start of each school year.

17. Incident Reporting, e-Safety Incident Log & Infringements

17.1 **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 SecureID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to a member of the Senior Leadership Team.

17.2 **e-Safety Incident Log -** The eS-afety Coordinator keeps a log of any e-Safety concerns or breaches. All incidents or concerns must be reported to the e-Safety coordinator.

17.3 **Complaints -** Complaints and/ or issues relating to e-Safety should be made to the e-Safety co-ordinator or Headteacher. Incidents should be logged by the e-Safety coordinator.

17.4 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

17.5 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, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

17.6 Staff are made aware of sanctions relating to the misuse or misconduct.

18. Internet Access

18.1 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. Whenever any inappropriate use is detected it will be followed up.

18.2 St John the Baptist C of E Primary School provides children access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.

18.3 Staff will preview any recommended sites before use.

18.4 Raw image searches are discouraged when working with pupils.

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

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

18.7 Staff must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise the intended restricted audience.

18.8 Staff should not reveal names of pupils, staff or adults associated with the school or any other confidential information acquired through your job on any social networking site or blog.

18.9 On-line gambling or gaming is not allowed.
It is at the Headteacher's discretion as to what internet activities are permissible for staff and pupils and how this is disseminated.

18.10 St John the Baptist C of E Primary School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; Data Protection Act 1998, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

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

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

18.13 The school uses management control tools for controlling and monitoring workstations in the ICT suite.

18.14 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.

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

18.16 Pupils and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility nor the network manager's to install or maintain virus protection on personal systems. **If pupils wish to bring in work on removable media it must be given to the ICT Technician for a safety check first.**

18.17 Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the ICT Subject Leaders.

18.18 If there are any issues related to viruses or anti-virus software, the network manager should be informed via telephone, email or ICT incident log.

19. Managing other web technologies

19.1 Social media including social networking sites, if used responsibly both outside and within an educational context can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

19.2 At present, the school endeavours to deny access to social networking sites in school.

19.3 All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.

19.4 Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

19.5 Pupils are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests).

19.6 Our pupils are advised to set and maintain their online profiles on such sites to maximum privacy and deny access to unknown individuals.

19.7 Pupils are encouraged to be wary about publishing specific and detailed private details and thoughts online.

19.8 Our pupils are asked to report any incidents of Cyberbullying to the school.

19.9 Staff may only create blogs, wikis or other online areas in order to communicate with pupils using the school website or other systems approved by the Headteacher.

20. Parental Involvement

20.1 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 along with the associated risks.

20.2 Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to St John the Baptist C of E Primary School

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

21. Passwords and Password Security

21.1 **Staff will always use their own personal passwords for e-mails, but a school password to access any computer.**

21.2 Staff will make sure they enter their personal passwords each time they logon. They will not include passwords in any automated logon procedures.

21.3 Staff should change temporary passwords at first logon.

21.4 Staff should change passwords whenever there is any indication of possible system or password compromise.

21.5 **Staff will only disclose their personal password to authorised ICT support staff when necessary, and never to anyone else**. They will ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

21.6 User ID and passwords for staff and pupils who have left the school are removed from the system by the ICT Technician.

21.7 **If you think your password may have been compromised or someone else has become aware of your password report this to your ICT support team**

22. Personal or Sensitive Information

22.1 Staff will: Ensure that any school information accessed from their own PC or removable media equipment is kept secure.

22.2 Ensure that they lock their screen before moving away from the computer during a normal working day to prevent unauthorised access.

22.3 Ensure the accuracy of any personal, sensitive, confidential and classified information they disclose or share with others

22.4 Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.

22.5 Ensure the security of any personal, sensitive, confidential and classified information contained in documents they fax, copy, scan or print.

22.6 Ensure that they only download material that is permissible.

22.7 Not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.

22.8 Keep the screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential or classified information.

22.9 Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

23. Storing/Transferring Personal, Sensitive, Confidential or classified Information Using Removable Media

23.1 Ensure removable media is purchased with encryption (Each member of staff is provided with a password protected memory stick for this purpose).

23.2 Store all removable media securely.

23.3 Securely dispose of removable media that may hold personal data.

23.4 Encrypt all files containing personal, sensitive, confidential or classified data.

23.5 Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

24. Remote Access

24.1 Staff are responsible for all activity via their remote access facility.

24.2 Staff will only use equipment with an appropriate level of security for remote access.

24.3 To prevent unauthorised access to school systems, staff must keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and not disclose them to anyone.

24.4 Select PINs to ensure that they are not easily guessed, e.g. do not use a house or telephone number or choose consecutive or repeated numbers.

24.5 Staff should avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

24.6 Staff must protect school information and data at all times, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

25. Use of Photos and Videos

25.1 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.

25.2 With the written consent of parents and staff, the school permits the appropriate taking of images by parents for specific events, with permission from the Headteacher (eg. School performances, Sports Day etc.).

25.3 The school will comply with Copyright laws which may restrict the taking of images for licensed events (e.g. Productions).

25.4 With written consent of parents, images may be published on school letters, newspapers, school website, programmes etc, as well as being available to purchase by parents.

25.5 Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

25.6 Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of others, unless given express permission by the Headteacher.

25.7 Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication.

26. Publishing Pupils Images

26.1 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)

26.2 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.

26.3 Parents or carers may withdraw permission, in writing, at any time.
E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

27. Storage of Images

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

27.1 Pupils and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Headteacher.

27.3 Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

27.4 The ICT Technician has the responsibility of deleting the images when they are no longer required, or when the pupil has left the school.

28. Webcams

28.1 We do not use publicly accessible webcams in school.

28.2 Webcams in school are only ever used for specific learning purposes.

28.3 Misuse of the webcam by any member of the school community will result in sanctions

29. Video Conferencing

29.1 Permission is sought from parents and carers if their children are involved in video conferences.

29.2 Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.

29.3 All pupils are supervised by a member of staff when video conferencing.

29.4 All pupils are supervised by a member of staff when video conferencing with end-points beyond the school.

29.5 The school keeps a record of video conferences, including date, time and participants.

29.6 Approval from the Headteacher is sought prior to all video conferences within school.

29.7 The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.

29.8 No part of any video conference is recorded in any medium without the written consent of those taking part.

30. ICT Equipment

30.1 **As a user of the school ICT equipment, staff are responsible for their own activity.**

30.2 The school will log ICT equipment issued to staff and record serial numbers as part of the school's inventory.

30.3 Visitors are not allowed to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.

30.4 Staff will ensure that all ICT equipment that they use is kept physically secure.

30.5 Staff will not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files or data. This is an offence under the Computer Misuse Act 1990.

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

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

30.8 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.

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

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

30.11 **It is the responsibility of staff to ensure that any information accessed from their own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.**

30.12 All ICT equipment allocated to staff must be authorised by the ICT Coordinators who are responsible for:

- maintaining control of the allocation and transfer within their unit
- recovering and returning equipment when no longer needed

30.13 ll redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

31. Portable and Mobile ICT Equipment

This section covers such items as laptops, mobile devices and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data

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

31.2 Staff must ensure that all school data is stored on the school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted.

31.3 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.

31.4 Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.

31.5 Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

31.6 The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.

31.7 In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

31.8 Portable equipment must be transported in its protective case if supplied.

32. Mobile Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such as portable media players, Smartphones, Blackberries, iPads, PDAs, games players are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

32.1 Personal Mobile Devices (including Smartphones)

- Pupils are allowed to bring personal mobile devices/phones to school but they must be handed to the school office for secure keeping until the end of the school day. At all times the device must be switched off or on silent. Parents must sign a permission slip before they can do this.

- The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

32.2 School Provided Mobile Devices (including phones)

- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on the devices of any member of the school community.
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.

33. Removable Media

33.1 Always consider if an alternative solution already exists

33.2 Only use recommended removable media

33.3 Encrypt and password protect

33.4 Store all removable media securely

33.5 Removable media must be disposed of securely by your ICT support team

34. Servers

34.1 The server will always keep in a locked and secure environment.

34.2 Access to the server is limited to the ICT Technician and ICT subject leader.

34.3 The server is password protected.

34.4 Existing servers have security software installed appropriate to the machine's specification.

34.5 Back up tapes are encrypted by appropriate software.

34.6 Data is backed up daily.

34.7 Back up tapes/discs are securely stored in a fireproof container.

34.8 Back up media stored off-site is secure.

35. Social Media Including Facebook and Twitter

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives. With regards to the use of social networking sites St John the Baptist C of E Primary School adheres to the following guidelines:

- Staff **are not permitted** to access social networking sites using school equipment in or out of school premises except for its own Twitter page found on the school's website
- Pupils **are not permitted** to access their social media accounts whilst at school.
- Staff, governors, pupils, parents and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.
- Staff, governors, pupils, parents and carers are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Staff, governors, pupils, parents and carers are aware that their online behaviour should at all times be compatible with the law.
- Children are taught that most social media sites are for those users above the age of 13 and the reasons for this. However, due to some children being allowed to sign up for these sites regardless, children at St John the Baptist C of E Primary School are taught about how to use these types of sites safely and responsibly as part of the e-Safety curriculum.

36. Systems and Access

36.1 Staff are responsible for all activity on school systems carried out under any access/account rights assigned to them, whether accessed via school ICT equipment or their own PC.

36.2 Staff must not allow any unauthorised person to use school ICT facilities and services that have been provided to them.

36.3 Staff will use only their own personal logons, account IDs and passwords and will not allow them to be used by anyone else.

36.4 Staff must keep their screen display out of direct view of any third parties when they are accessing personal, sensitive, confidential or classified information.

36.5 Staff should ensure that they lock the screen before moving away from the computer during a normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.

36.6 Staff should ensure that they logoff from the PC completely when they are going to be away from the computer for a longer period of time.

36.7 Staff will not introduce or propagate viruses.

36.8 It is imperative that users do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability

Discrimination Act).

36.9 Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.

36.10 Where necessary, staff will obtain permission from the owner or owning authority and pay any relevant fees before using, copying or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

36.11 It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever the school appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

37. Telephone Services

37.1 Staff may make or receive personal telephone calls using the school telephone provided:

1. They are infrequent, kept as brief as possible and do not cause annoyance to others.

2. They are not for profit or to premium rate services.

3. They conform to relevant school policies.

37.2 School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.

37.3 Staff are aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

37.4 Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat.

38. Personal Mobile Phones

38.1 Staff are responsible for the security of personal mobile phones whilst in school. Always set the PIN code on your mobile phone and do not leave it unattended and on display (especially in vehicles).

38.2 Staff will report the loss or theft of any personal mobile phone equipment immediately.