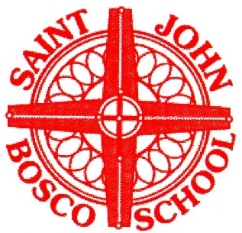
**St John Bosco RC Primary School**

With Jesus in our hearts, we love, pray, learn and play.

**E-safety policy**

**1. Introduction**

The use of technology is widespread throughout daily life. Education is no different and there are various forms of technology in use within the school. This policy aims to set out the safe use of technology by pupils and staff and the procedures for managing this.

**2. Ethos and Values**

At St. John Bosco we are committed to using technology to enhance and enrich the teaching and learning experience throughout the school. In doing this we aim to educate pupils in the benefits of using technology but also to understand its weaknesses and potential danger. Children have a right to information (Article 13 UNCRC) and a right to privacy (Article 16 UNCRC).

In order to facilitate the safe use of technology a number of preventative measures have been taken. The safe use of technology however is not a Computing issue but a safeguarding issue and the content of this policy reflects this.

**3. Aims and Objectives**

We aim to use technology in daily life at St. John Bosco to make learning relevant, enjoyable and challenging.

We seek to do this by:

* Making the most of the technology and the resources that the internet provides by using it:
  + As a research tool
  + As a source of learning activities
  + To share what we have learnt with others in our school
  + To provide information to parents and the wider community
* Providing software which is relevant to the curriculum and is challenging and rewarding
* Using still photography and video:
  + As an information source
  + To celebrate and record what we have achieved

**4. Roles and Responsibilities**

4.1 The Headteacherwill ensure that:

* All staff should be included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action and possible dismissal.
* All staff know to log e-safety concerns about children using CPOMS.
* A Designated Senior Member of Staff for E-Learning/Safety is identified and receives appropriate on-going training including training which promotes awareness of the risks posed by the internet and mobile technology, how to deal with incidents including escalation and reporting, support and supervision and works closely with the Designated Person for Safeguarding.
* All temporary staff and volunteers are made aware of the school’s E-Learning/Safety Policy and arrangements (outlined in the school’s Safeguarding Policy)
* A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

4.2 The Governing Body of the school will ensure that:

* There is a senior member of the school’s leadership team who is designated to take the lead on E-Learning/Safety within the school
* Procedures are in place for dealing with breaches of e-safety and security and are in line with Local Authority procedures
* All staff and volunteers have access to appropriate Computing training.

4.3 The Designated Senior Member of Staff for E-Learning/Safety will:

* Liaise with the Designated Person for Safeguarding as appropriate
* Ensure that IT security is maintained
* Attend appropriate training
* Provide support and training for staff and volunteers on E-Safety
* Ensure that a copy of the school’s Acceptable Use Policy is signed by all staff and available to volunteers
* Ensure that the school’s IT systems are regularly reviewed with regard to security
* Ensure that the virus protection is regularly reviewed and updated

4.4 Staff working with children through training will be made aware of:

* The risks posed by the online world
* Possible warning signs
* Where to go if an incident occurs and how this links to safeguarding procedures (including logging on CPOMS)
* Professional standards and protecting themselves (for example not friending children on social networking sites)
* School policies on the use of personal devices (for example phones/cameras)

All technologies used in school are identified and the following measures are put in place to try and pre-empt e-safety risks before they occur.

**5. Internet Use**

Pupils and teachers access the internet regularly as part of the day to day teaching and learning experience. The following measures exist to ensure that this happens in a safe and controlled manner:

* Internet access will be filtered with access to unsuitable sites being blocked
* Access to internet social networking sites will not be allowed
* Pupil access to the internet will be supervised at all times
* Pupils and staff will report any unsuitable sites using the appropriate procedure

**6. School Website**

The school uses its website to communicate news, events and successes to parents, carers and the wider community. The following measures exist to ensure that this happens in a safe and controlled manner:

* Editorial guidance will ensure that the school’s ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material
* The Headteacher will have overall editorial responsibility and ensure that all content is accurate and appropriate
* Photographs of pupils will not be published without the consent of parents
* The names of children will not be published alongside photographs.

**8. Photography and Video**

Photographs and Videos are used within the school to record success and to celebrate what we have achieved. The following measures exist to ensure that this happens in a safe and controlled manner:

* Photographs and video will be taken with care to ensure that pupils within them cannot be easily identified or the images misused
* Photographs and video will not be published online without parental permission
* Photographs and videos will not be referenced online with file names which identify the individuals within them.

**Use of digital and video images - Photographic, Video**

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff and pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

* When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
* Staff are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes
* Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
* Pupils must not take, use, share, publish or distribute images of others without their permission
* Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with GDPR with regards the use of such images.
* Students’ / Pupils’ full names will not be used anywhere on a website or blog, particularly in association with photographs.
* Permission from parents or carers will be obtained before photographs of pupils are published on the school website via our online permissions form.
* Pupil’s work can only be published with the permission of the pupil and parents or carers

When using communication technologies the school considers the following as good practice:

* The official school email service is regarded as safe and secure and is monitored.
* Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems
* Users need to be aware that email communications may be monitored
* Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
* Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content
* Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material
* Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

**Storage of Images**

Images/ films of children are stored securely on the school server, school livedrive and dropbox account or teacher’s individual school laptops.

**9. Mobile Phones and Personal Photography**

Pupils who are responsible for making their own way home or who may need a mobile phone after the end of the school day are permitted to bring a phone with them to school. Parents must complete an Acceptable use of a mobile phone agreement (Appendix 3). The phone must be handed in as requested on entering the school building and must be switched off whilst on school premises. The use of mobile phones by pupils on school premises is not permitted. The ability to bring a mobile phone into school is a privilege which may be withdrawn if pupils fail to follow these guidelines. This privilege may be withdrawn at any time at the discretion of the Headteacher.

Children are not permitted to take digital photographs or videos using personal devices anywhere on the school premises.

**10. Personal Mobiles – Staff**

• Staff are not permitted to make/receive calls/texts during contact time with children. Emergency contact should be made via the school office and/or via landlines located in each Faculty or by walkie-talkies where provided. If you are in a location where communication is not possible (e.g. fields, woods, astro) and you do not have a walkie-talkie then staff should carry mobile phones for emergency use only.

• Staff should have their phones on silent or switched off and out of sight (eg in a drawer, handbag) during class time.

• Mobile phones should not be used in a space where children are present (eg classroom, corridor, playground).

**Mobile Phone Policy**

• Use of phones (including receiving/sending texts and emails) should be limited to non-contact time when no children are present e.g in office areas, staff room, empty classrooms.

• Staff must security protect access to their phone.

• Should there be exceptional circumstances (e.g acutely sick relative), then staff should make the Headteacher and office staff aware of this so messages can be relayed promptly.

• Staff are not at any time permitted to use recording equipment on their mobile phones, for example: to take recordings of children, or sharing images. Legitimate recordings and photographs should be captured using school equipment such as cameras, ipads or school phones.

• Staff should report any usage of mobile devices that causes them concern to the Headteacher.

**Mobile Phones for work related purposes**

We recognise that mobile phones provide a useful means of communication on off-site activities. However, staff should ensure that:-

• Mobile use on these occasions is appropriate and professional (and will never include taking photographs of children)

• Mobile phones should not be used to make contact with parents during school trips – all relevant communications should be made via the School Office.

• Where parents are accompanying trips they are informed to keep their phones on silent, not to make contact with other parents (via calls, text, email or social networking) during the trip or use their phone to take photographs of children.

**11. Social Networking**

The school does not permit the pupils to access their private accounts on social or gaming networks at any time during the school day.

The school also strongly discourages children from using age inappropriate social networking outside of school. Should the staff be made aware of incidents or activities on these social networks, which has a direct effect on the children’s behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child’s access to the respective organisations/companies.

**12. Network Security**

Access to the schools computers, the internet and data are controlled by network login.

* Pupils access the school network using a generic login and password for their year group. Pupil login provides them with access to the internet as described above, controlled access to software and access to their year group folder where they can save and retrieve files.
* Staff access the school network using personal login id and password. Staff login provides them with access to the internet as described above, controlled access to software and access to their personal folder where they can save and retrieve files.
* The network server and all computers within the school have anti-virus software installed which is updated on a regular basis.
* Access to new or temporary members of staff will be authorised by the Headteacher.
* A guest login and laptop is available with restricted access to enable supply teachers and other visitors to prepare lessons or show presentations.

**13. Data Security**

All data is held on the academic or administration server, both of which have backups taken on a regular basis. No data is held on individual computers. All staff laptops are encrypted. Data on these machines cannot be accessed without the password. Where there is a requirement to access sensitive data off-site and an encrypted laptop is not available, such data off will be stored on an encrypted USB memory stick.

Staff may store non-sensitive data on unencrypted USB memory sticks.

Staff are responsible for ensuring that USB sticks are only used in computers which have adequate up to date anti-virus software.

Pupils may not use USB memory sticks without the permission of a teacher.

**14. Installation of Software**

Any new software required to be installed on to schools computers will be reviewed by the Computing Co-ordinator / IT Technician. Staff and Pupils will not have access to install software. Installing and downloading software may only be done by a System Administrator.

Staff are permitted to download Apps on to their staff iPads as long as they are free and appropriate (see Acceptable Use Policy). Staff must not download any Apps that cost money unless it has been agreed with the Computing co-ordinator).

**15. Acceptable Use Policy**

All Staff, Key Stage 2 pupils and parents of pupils in the Early Years and KS1 will be asked to agree to and sign, the acceptable use agreement (see Appendix 1 - AUA). Parents will also be offered advice on where to find help or additional information on e-safety issues (see Appendix 2).

**16. E-Safety Curriculum**

The school recognises the opportunities and potential threats that the use of technology brings.

The breadth of issues classified within E-Safety is considerable, but can be categorised into four areas of risk:

**Content** – being exposed to illegal, inappropriate or harmful content.

**Contact** – being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children with the intention to groom or exploit them.

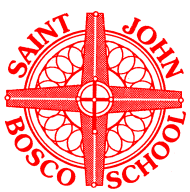
**Conduct** – personal online behaviour that increases the likelihood of or causes harm, for example, making and sending and receiving inappropriate messages and online bullying.

**Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

To enable the children to maximise the potential of technology in a safe and effective way, e-safety is regularly taught to ensure children know what safe practice is and how to deal with situations that make them feel uncomfortable online. Children have a right to information (Article 13 UNCRC) and a right to privacy (Article 16 UNCRC) and children’s rights are included in e-safety teaching. We have digital Leaders who have been trained to promote e-safety across school through a variety of activities including posters, assemblies, leaflets and visiting classes.

E-safety is taught using the SMART acronym: stay SAFE by keeping personal information private; MEETING people you only know from online can be dangerous; ACCEPTING unknown files from people you don’t know or trust can lead to problems such as viruses; information on the internet is not always RELIABLE; and TELL a trusted adult if anything you see online makes you feel uncomfortable including cyberbullying.

Updated September 2021

**Appendix 1 – Acceptable Use Agreements**

**St John Bosco RC Primary School**

**Computer and Internet Use Agreement - Pupils**

|  |  |
| --- | --- |
| **Acceptable use of the school’s ICT facilities and internet: agreement for pupils and parents/carers** | |
| **Name of pupil:** | |
| **When I use the school’s ICT facilities (like computers and equipment) and get on the internet in school, I will not:**   * Use them without asking a teacher first, or without a teacher in the room with me * Use them to break school rules * Go on any inappropriate websites. * Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson) * Use chat rooms * Open any attachments in emails, or click any links in emails, without checking with a teacher first * Use mean or rude language when talking to other people online or in emails * Share my password with others or log in using someone else’s name or password (for example Purple Mash or TT Rockstar) * Bully other people * Will follow SMART to help us stay safe online * Will treat all computer equipment (including cameras, laptops and iPads) with care and respect * Never share personal information about ourselves or others when on-line   I understand that the school will check the websites I visit and how I use the school’s computers and equipment. This is so that they can help keep me safe and make sure I’m following the rules.  I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.  I will always be responsible when I use the school’s ICT systems and internet.  I understand that the school can discipline me if I do certain unacceptable things online, even if I’m not in school when I do them. | |
| **Signed (pupil):** | **Date:** |
| **Parent/carer agreement:** I agree that my child can use the school’s ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school’s ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these. | |

**Parents to indicate agreement via the school permissions form.**

**Computer and Internet Use Agreement – Pupils**

**Foundation Stage and Key Stage 1**

These rules help us to stay safe on the internet

* We will only use the internet when an adult is with us
* We can click on the buttons or links when we know what they do
* We can search the internet with an adult
* We always ask if we get lost on the internet
* We tell an adult if we see anything we are uncomfortable with
* We will follow SMART to help us stay safe online

**Key Stage 2**

E-safety rules for Key Stage 2

* We will treat all computer equipment (including cameras, laptops and iPads) with care and respect
* We will only use computers or iPads if we have the permission of a teacher. We will only use a specific numbered device, unless permission is given by an adult to use an alternative.
* We never share our username or password with anyone else (for example Purple Mash)
* We never share personal information about ourselves or others when on-line
* We only access the internet if we have the permission of a teacher
* We tell an adult if we see anything that we are uncomfortable with
* We only search for sites and information which relate to school activities
* We will only use activities directed by an adult.
* We will enable adults to see what we are doing when requested.
* We will follow SMART to help us stay safe online

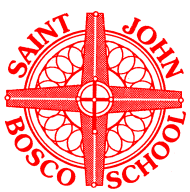
**St John Bosco RC Primary School**

**E-safety rules**

All pupils use computer facilities including internet access as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-safety rules relevant to their Key Stage have been understood and agreed.

|  |  |
| --- | --- |
| Pupil: | Class: |
| **Pupil’s agreement**   * I have read and I understand the school e-safety rules * I will use the computer, network, internet access and new technologies in a responsible way at all times * I know that the network and internet access may be monitored * I understand that if I do not follow these rules I will be dealt with according to our school behaviour policy. | |
| **Children to agree during discussion in classroom.** | |
| **Parental consent**   * I have read and understood the school e-safety rules and give permission for my child to access the internet. * I understand that the school will take all reasonable action to ensure that pupils cannot access inappropriate materials but acknowledge that incidents beyond school’s control can occur. * I understand that through the e-safety curriculum the children will learn how to respond should this happen and I support school in delivering this. | |

**Parents to indicate agreement via the school permissions form.**

**St John Bosco RC Primary School**

**Computer and Internet Use Agreement – Staff**

|  |
| --- |
| **Acceptable use of the school’s ICT facilities and the internet: agreement for staff, governors, volunteers and visitors** |
| **Name of staff member/governor/volunteer/visitor:** |
| When using the school’s ICT facilities and accessing the internet in school, or outside school on a work device, I will not:   * Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) * Use them in any way which could harm the school’s reputation * Use any improper language when communicating online, including in emails or other messaging services * Install any unauthorised software, or connect unauthorised hardware or devices to the school’s network * Share my password with others or log in to the school’s network using someone else’s details * Share confidential information about the school, its pupils or staff, or other members of the community * Access, modify or share data I’m not authorised to access, modify or share * Promote private businesses, unless that business is directly related to the school * I will check that anti-virus protection is up to date on my laptop and will report any problems with this. If my computer indicates that there is an infection by a virus I will stop using it immediately and bring it into school for assessment * I am aware of and will follow the school ‘Social Networking Policy’ in relation to use of school computer equipment * I will only store work-related files on my laptop and iPad |
| I understand that the school will monitor the websites I visit and my use of the school’s ICT facilities and systems.  I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school’s data protection policy.  I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.  I will always use the school’s ICT systems and internet responsibly, and ensure that pupils in my care do so too. |
|  |

**Computer and Internet Use**

* I will keep my laptop encryption password, iPad login and laptop/network login password private at all times
* I will not use the internet for any activities which may be considered to be inappropriate
* If I access material on this computer which is inappropriate I will inform the Computing Co-ordinator or a member of the Senior Leadership Team as soon as possible with the details of the website and its address (url)
* I will check that anti-virus protection is up to date on my laptop and will report any problems with this. If my computer indicates that there is an infection by a virus I will stop using it immediately and bring it into school for assessment
* I am aware of and will follow the school ‘Social Networking Policy’ in relation to use of school computer equipment
* I will only store work-related files on my laptop and iPad

**Staff – to login into CPOMS documents and “mark as actions” to show their agreement.**

**Appendix 2 – Further advice**

**CEOP** – Child Exploitation Online Online Protection Centre [www.ceop.police.gov.uk](http://www.ceop.police.gov.uk)

**Think U Know** resources for teachers, trainers and children [www.thinkuknow.co.uk](http://www.thinkuknow.co.uk)

**Digizen** - Information on Cyberbullying and Social Networks [www.digizen.org](http://www.digizen.org)

**Beat Bullying (formerly Cybermentors)** - Staffed by trained YP, Beat Bullying provide a service to support and listen to YP who are being bullied. The cybermentors are supported by BACP accredited counsellors. <http://www.beatbullying.org/>

**IWF** – The Internet watch Foundation is the UK internet Hotline for the public and IT professionals to report criminal online content in a secure and confidential way. [www.IWF.org.uk](http://www.IWF.org.uk)

**MSCB Sexting Guidance Document** – Additional guidance for understanding and responding to incidents where young people create and / or circulate indecent images of themselves / other young people

**Online Safety Compass** - Online Compass is a free online safety self-review tool for any group that works with children and young people. [www.onlinecompass.org.uk/](http://www.onlinecompass.org.uk/)

**Professionals Online Safety Helpline -** Free advice for professionals working with children and young people on all areas of online safety. [www.saferinternet.org.uk/helpline](http://www.saferinternet.org.uk/helpline)

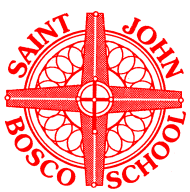
**UK Safer Internet Centre** - The latest advice on how to use the internet and new technologies safely and responsibly. Also find a range of practical resources, news and events focussing on the safe and responsible use of the internet and new technologies. [www.saferinternet.org.uk/](http://www.saferinternet.org.uk/)

**360 Degree Safe** - The 360 degree safe self-review tool is currently available free of charge and is intended to help schools review their e-safety policy and practice - [www.360safe.org.uk/](http://www.360safe.org.uk/)

**Childnet** – Childnet is a non-profit organisation working with others to protect children online. Our school works with them to train our Digital Leaders - [www.childnet.com](http://www.childnet.com)

**Appendix 3 – Acceptable use of mobile phone agreement**

St. John Bosco R.C. Primary School

****

**Acceptable use of a mobile phone agreement**

Pupils are permitted to bring a mobile phone to school, to support safety issues if they come to school independently or to contact parents after school. All mobile phones should be handed into the school office at the beginning of the day and collected at the end of the day.

If parents want their child to bring a phone it is on the understanding that they agree with the following conditions:

* the phone will be kept in the main school office during the day
* mobile phones must be switched off at all times during the school day, including break and lunchtimes, and remain off whilst pupils are on the school premises
* It is not permitted to film or photograph anyone on school grounds
* content on the phone (e.g. messages, emails, pictures, videos, sound files) will be shown to a teacher if requested.

**Misuse of phones**

Parents are notified that appropriate action will be taken against those who are in breach of the acceptable use guidelines following the schools discipline and behaviour policy.

In the case of misuse the phone will only be returned to a parent/carer who will be required to visit the school to collect the phone.

Serious misuse may lead to the confiscation of the mobile phone, communication with parents and the imposition of other sanctions, up to and including exclusion from school. In some instances, an offence may have to be reported to the Police.

**Parents to indicate agreement via the school permissions form.**