St. John Bosco RC Primary School

E-Safety Policy

CONTENTS

E-SAFETY POLICY

Introduction

E-Safety encompasses the use of new technologies, internet and electronic communications such as mobile phones, email , social networking, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

End to End e-Safety

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies
- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use
- Safe and secure broadband Network including the effective management of filtering.
  National Education Network standards and specifications.

School e-safety policy

Writing and reviewing the e-safety policy

The e-Safety Policy has been reviewed and updated to reflect the need to raise awareness of the safety issues associated with electronic communications as a whole.

1. TEACHING AND LEARNING

Why Internet use is important

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.

- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Internet use will enhance learning
- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be taught how to evaluate Internet content.
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

2. MANAGING INTERNET ACCESS

Information system security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection is updated regularly.
- Security strategies will be regularly reviewed

3. E-MAIL

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

4. PUBLISHED CONTENT AND THE SCHOOL WEB SITE

The contact details on the website should be the school address, e-mail and telephone number.
Staff or pupils' personal information will not be published.
The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
St. John Bosco RC Primary School values the contribution that a website can make to the life and role of the school in a modern society. Our school website has 5 important roles:

1. *To promote the school*
2. *To provide information to prospective parents and teachers, the wider community and the world*
3. *To act as a communication channel between teachers, parents, pupils and school management*
4. *To improve pupil learning*
5. *To raise standards in teaching and learning.*

5. SAFEGUARDING

The safety of children and other users who appear or are referred to on the published site is of paramount importance.

Publishing names, images and work

- Adult's names will be published as their title and last name e.g. Mrs Smith.
- It is the policy of the school to not allow children's surnames or for any photographs which clearly identify any children to be used on the website without the parents/carers permission.
- Children will only be shown in photos where they are suitably dressed.
- Personal details of children, staff and governors, such as home addresses, telephone numbers, personal e-mail addresses, etc, will not be released via the website or school e-mail.

Privacy

- Adults have the right to refuse permission to publish their image on the published site.
- Parents have the right to refuse permission for their child's work and/or image to be published on the published.

Those wishing to exercise this right should express their wishes in writing to the Headteacher, clearly stating whether they object to work, images, or both being published, to the published site or extranet. Parents will be notified of this right by publication of this policy on an annual basis.

Any persons named on a web page can ask for their details to be removed. The web pages will be regularly reviewed for accuracy and will be updated as required. This review will occur at least annually.

Social networking and personal publishing

- The school will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- The school does not currently have a Twitter of Facebook account.
- Pupils and parents will be advised that the use of social network spaces outside school is considered inappropriate for primary aged pupils to use unsupervised. School staff have been instructed not to allow parents or children under 16 to be accepted as their 'friends' on any site.
-

6. MANGEMENT

Managing filtering

The school will work with the LA, DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
If staff or pupils discover an unsuitable site, it must be reported to the ICT/ e-Safety Coordinator.

Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

7. POLICY DECISIONS

Authorising Internet access

Access to the Internet will be under adult supervision to access specific, approved on-line materials.

Assessing risks

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences of Internet access.
The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Advice would be sought from the LA/Diocese in the event the school needed to establish procedures for handling potentially illegal issues.

Community use of the Internet

The school will liaise with local organisations to establish a common approach to e-safety.
External organisations using the school's ICT facilities must adhere to the e-safety Policy.

8. COMMUNICATIONS POLICY

Introducing the e-safety policy to pupils

E-safety rules will be posted in all classrooms and discussed with the pupils at the start of each year.
Pupils will be informed that network and Internet use will be monitored.

Staff and the e-Safety policy

All staff will be given the School e-Safety Policy and its importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

A laptop issued to a member of staff remains the property of the school. Users of such equipment should therefore adhere to school policy regarding appropriate use with regard to Internet access, data protection and use of software

Enlisting parents' support

Parents' attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus, and school website.

Mobile phones will not be used during lessons or formal school time. They must be handed into the school office at the start of the school day and collected at the end of the school day. The sending of abusive or inappropriate text messages is forbidden.

9. MONITORING AND REVIEW

- Our e-Safety Policy has been agreed by senior management and approved by governors.
- The e-Safety Policy and its implementation will be reviewed biannually unless changes to legislation demand otherwise.
- This policy is implemented on a day-to-day basis by all school staff and is monitored by the e-safety Co-ordinator.
- This policy is the Governors' responsibility and they review its effectiveness annually.

Signed: _____

Designation: _____

Date: _____

Review Date: _____