CROSS AND PASSION COLLEGE E-SAFETY POLICY 2016-2017

1 WRITING AN REVIEWING THE E-SAFETY POLICY

The E-Safety Policy is part of the School Development Plan and relates to other policies including those for ICT, bullying and for Child Protection.

This policy has been created using the **BECTA E-Safety Guidelines**

2 TEACHING AND LEARNING

2.1 Why ICT Access is Important

- Internet and emerging communication technologies are essential elements in 21st century life for education, business and social interaction. Our school has a duty to provide students with quality access as part of their learning experience.
- Information Communication Technologies access is an essential part of the curriculum and a necessary tool for staff and pupils.

2.3 Information Communication Technologies Use Should Enhance Learning

- The school Information Communication Technologies access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.

  Pupils are taught what Information Communication Technologies use is acceptable and what is not and are given clear objectives for Information Communication Technologies use.
- Pupils are educated in the effective use of the Information Communication Technologies in research, including the skills of knowledge location, retrieval and evaluation

2.4 Pupils are taught how to evaluate Information Communication Technologies content

- The school ensures that the use of Information Communication Technologies derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.

3 MANAGING INFORMATION COMMUNICATION TECHNOLOGIES ACCESS

3.1 Information System Security

School ICT systems capacity and security are reviewed regularly in consultation with C2k.

3.2 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.
- An 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.

3.3 Published Content and the School Web Site

- The contact details on the school web site show the school address, e-mail and telephone number. Staff or pupils' personal information are not published.
- The Principal takes overall editorial responsibility and ensures that content is accurate and appropriate.

3.4 Publishing Pupils' Images and Work

- Photographs that include pupils are selected carefully and should not enable individual pupils to be clearly identified.
- Pupils' full names should not be used anywhere on the web site or Blog, particularly in association with photographs.
- Written permission from parents or carers is obtained before photographs of pupils are published on the school web site.
- Pupil's work can only be published with the permission of the pupil and parents/carers.

3.5 Social Networking and Personal Publishing

- The school blocks/filters access to social networking sites.
- Newsgroups are blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind which may identify them or their location.

3.6 Managing Filtering

- Our school works with the NEELB, C2k, DTI and the Information Communication Technologies 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 E-Safety Coordinator – Mr C Nugent.
- The E-Safety Coordinator and the IT Technician make regular checks to ensure that the filtering methods selected are appropriate, effective and reasonable.

3.7 Managing Videoconferencing

- IP videoconferencing uses the educational broadband network to ensure quality of service and security rather than the Information Communication Technologies.
- Pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing is appropriately supervised for the pupils' age.

3.8 Managing Emerging Technologies

- Emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- Mobile phones should not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff should be issued with a school phone where contact with pupils is required.

3.9 Protecting Personal Data

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

4 POLICY DECISIONS

4.1 Authorising Information Communication Technologies Access

- All members of staff and pupils must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- Parents will be asked to sign and return a consent form.

4.2 Assessing Risks

- The school takes all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Information Communication Technologies content, it is not possible to guarantee that unsuitable material should never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Information Communication Technologies access.

- Our school audits ICT provision to establish if the E-Safety Policy is adequate and that its implementation is effective.

4.3 Handling E-Safety Complaints

- Complaints of the misuse of Information Communication Technologies are addressed by the E-Safety Coordinator/senior member of staff.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents are informed of the complaints procedure.
- Discussions should be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

5 COMMUNICATING THE POLICY

5.1 Introducing the E-Safety Policy to Pupils

- E-safety rules are posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils are informed that network and Information Communication Technologies use are monitored.
- Year 8 Pupils are taught a unit on E-Safety

5.2 Staff and the E-Safety Policy

- All members of staff are given the School E-Safety Policy and its importance explained.
- Staff should be aware that Information Communication Technologies traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

5.3 Enlisting Parents' Support

- Parents' attention is drawn to the School E-Safety Policy in newsletters, the school prospectus and on the school Web site.

REVIEW

Date policy implemented: **September 2016**

Review Date: **June 2018**