Saint Cecilia's Church of England School

INVESTORS IN PEOPLE | Silver

"Glorifying God though outstanding, enjoyable education"

E-Safety Policy

The Governing Body is committed to providing a safe and healthy workplace for all employees, pupils and students and to ensure that their work does not adversely affect the e-safety of other people.

E-Safety encompasses Internet Technologies and Electronic Communications such as Mobile Phones and Wireless Technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

Encouraging Effective e-Safety

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

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

Teaching and Learning

Why Internet Use is of Value in Education

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

The School Aims to Enhance Learning by….

- Designing Internet access that will be expressly for pupil use and will include filtering appropriate to the age of pupils.
- Teaching pupils aspects of Internet use that are acceptable and what is not, and given clear objectives for Internet use.
- Teaching pupils about the responsible use of emerging technologies (thus encouraging self-regulation) so that they may make informed choices
- Teaching pupils, effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Internet Content

- Schools should ensure that the use of Internet derived materials by staff and by pupils comply 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.

Managing Internet Access Information System Security

- School ICT systems capacity and security will be reviewed regularly by the Business Manager.
- Virus protection is installed and updated regularly.

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 at school.
- 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 where appropriate authorised before sending, in the same way as a letter written on school headed paper.
- The use of mass distribution lists should not be encouraged.
- If issues are sensitive, staff should always seek advice prior to sending email.

Published Content and the School Website

- 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 or Marketing Manager will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by name without permission.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Work can only be published with the permission of the pupil and parents.

Social Networking and Personal Publishing in School

- School will block/filter access to Social Networking Sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils should be advised on security and must set passwords and deny access to others. They must also be advised on how to block unwanted communications.
- Pupils and Students should be encouraged to invite known friends only and deny access to others.

Social Networking and Personal Publishing for External Use

- As the Social Network Space is public domain, pupils, students and staff must not post any information and comments that are derogatory to the school community.

Managing Filtering

The school will work in partnership 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 Innovit.

Managing Video-Conferencing, including use of Webcam

- IP video-conferencing 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 video-conference call.
- Video-conferencing will be appropriately supervised for the pupil's age.

Managing Emerging Technologies

- Emerging Technologies will be examined for educational benefit before use in school is allowed.
- The sending of abusive or inappropriate text and any social messaging using new technologies in school is forbidden.

Protecting Personal Data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Should any future communication with parents be by email, there will be protection of that data
- All data will be removed from redundant hard drives before their disposal.

Authorising and Controlling Internet Access

- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable

material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Communicating the e- Policy Introducing the e-safety policy to pupils

- 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.
- Staff that manage filtering systems or monitor ICT use will be supervised by Senior Management and have clear procedures for reporting issues.

Enlisting Parents' Support

- Parents' attention will be drawn to the School e-Safety Policy in Newsletters and on the school Website.

Further Information

e-Safety Policy Guidance http://www.kenttrustweb.org.uk//Children/safeguards_esafety.cfm

Safer Internet Centre www.saferinternet.org.uk