St Ethelbert’s Catholic Primary School
e-Safety Policy

“I serve Jesus with my body, heart, mind and soul.”

Serviam means ‘I serve’. Jesus Christ has taught us, ‘it is more blessed to serve than to be served’. At St Ethelbert’s school, following our Catholic faith, we serve the whole person – mind, heart, body and soul.

Body – because we care for our wellbeing, our parish neighbourhood and our environment.
Heart – because we teach love and respect for all.
Mind – because we believe in excellent education.
Soul – because we learn to pray and become closer to God as his children.

The Internet has become an integral part of children’s lives, enabling them to undertake research for school projects, talk to their friends and access information from around the world. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Increasing provision of the Internet in and out of schools brings with it the need to ensure that learners are safe. Unfortunately though, there are times when Internet use can have a negative effect on children. We should be aware of the potential dangers, taking measures to ensure safe usage by all. Internet safety requires a whole school approach and any teacher who uses ICT in the classroom, has a duty to ensure that children are regularly reminded about appropriate usage.

Authorising Internet access

- All staff must read and sign the ‘Acceptable ICT Use Agreement’ before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted Internet access.
- All staff will be alerted to the School’s e-safety policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Staff and pupil users will have their own usernames and password, which will enable monitoring of individual users.
- Parents will be asked to sign and return an Internet consent form upon their child’s admission to the school.

Internet Usage

- Internet access will be planned to enrich and extend learning activities.
- Access levels will reflect the curriculum requirements and age of pupils.
- Pupils will be taught what Internet use is acceptable and unacceptable and will be given clear objectives for Internet use.
- Pupils will be informed that Internet use will be monitored.
- Pupils will be supervised by an adult when using the Internet.
- An e-safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use. This will be part of our PSHE curriculum.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.

- At Key Stage 2, the focus will shift to children navigating the Internet themselves to find specific information, therefore requiring more accessibility.

System Security

Technology such as firewalls and filtering and monitoring software are an important aspect of safeguarding the school's computer networks. Internet filtering systems prevent or block users' access to unsuitable material. When the filtering system is turned on, users cannot open or link to sites that the filtering system recognises as unsuitable. Filtering is an effective tool, but it is important to remember that no filtering software is foolproof and should be combined with the full range of internet safety measures such as acceptable use policies, monitoring pupil activity, and education and awareness.

- The school uses the Kent Broadband with its firewall and filters appropriate to the age of pupils.
- School ICT systems capacity and security will be reviewed regularly by the contracted ICT technicians.
- Virus protection will be installed and updated regularly.
- The ICT subject leader and the contracted ICT technicians will review system capacity regularly.

E-mail

Staff and pupils will begin to use e-mail to communicate with others, to request information and to share information. When young people are using email, there is always a risk that they might receive unsuitable messages. Pupils should be taught the appropriate behaviours to adopt if they receive an inappropriate or offensive email, such as deleting the message, or closing it and seeking advice from their teacher, but never replying to it. This will allow the teacher to go back and check the message, talk through some of the issues, reassure the pupil that it was not their fault that they received such a message, and take any other action as appropriate.

- Pupils may only use approved e-mail accounts on the school system.
- For external e-mail, there is no need for pupils to use individual accounts. A class e-mail account will be set up and monitored by the teacher.
- Outside e-mail exchanges may be arranged as a class project.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils may only send e-mail as part of planned lessons and not at their leisure.
- In-coming e-mail to pupils will not be regarded as private.
- The forwarding of chain letters will not be permitted.
- Whilst in school, email will only be used for educational purposes. Pupils will not be allowed to access their personal mailboxes from the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils should be made aware of the characteristics of email bullying, the effects it can have on the recipient, and strategies for dealing with it.
- Parents, teachers and governors will be able to send and receive emails externally.
- Email attachments should always be treated with caution. A virus checker will be used on all outgoing and incoming email.

Social networking and personal publishing

- The 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 and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff or the ICT Subject Leader.
- Any complaint about staff or pupil misuse must be referred to the Head Teacher.
- Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable on the Internet.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the ICT Subject Leader.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Digital Photographs

- Staff will only use school authorised cameras and videos for recording children's educational activities.
- If staff have to use their own equipment in an emergency – then all photos should be copied to the school intranet as soon as possible and then deleted from personal equipment.

It is essential that all pupils are taught the relevant skills and strategies to remain safe when using such technologies. This should be as discrete e-safety lessons, and also as part of the ICT curriculum, or embedded within all curriculum work wherever it is relevant.

Written by Mr Joss

Review February 2019