CORPUS CHRISTI CATHOLIC PRIMARY SCHOOL

GOVERNORS POLICY FOR E-SAFETY

OUR MISSION STATEMENT

Christ is like a single body which has many parts.
'It is still one body even though it is made up of many parts.'
(1 Corinthians 12 : 12)

We are a community which supports children's learning and the development of their Catholic faith.

We witness this by recognising that Jesus is with us in all we think, do and say.

We acknowledge the challenge of every individual
and strive to enable them to develop their full potential.

Rationale:

The school has a duty of care to ensure that children are able to use the internet and related communications technologies appropriately and safely.
The purpose of this e-safety policy is to outline what measures the school takes to ensure that students can work in an e-safe environment and that any e-safety issue is detected and dealt with in a timely and appropriate fashion.

Aims:

- To offer equality of opportunity to all our pupils to access the Internet as a resource
- To give children experience of Internet use in a safe, secure context
- To raise educational standards through research skills

Objectives:

- To structure Internet use into curriculum planning
- To encourage children to validate information
- To set in place procedures and strategies allowing pupils to access the Internet safely
- To make children aware that the Internet is a valuable tool for communication and research, but one that has associated dangers.
- To work in partnership with parents, the DOSC, and the LA to ensure provision of systems that will protect all members of the school community.

Technologies
ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information. Current and emerging Internet and online technologies used in school and, more importantly in many cases, used outside of school by children include:

- The Internet – World Wide Web

- e-mail
- Instant messaging (often using simple web cams) e.g. Instant Messenger)
- Web based voice and video calling (e.g. Skype)
- Online chat rooms
- Online discussion forums
- Social networking sites (e.g. Facebook)
- Blogs, Vlogs and Micro-blogs (e.g. Twitter)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (e.g. You Tube)
- Music and video downloading (e.g. iTunes)
- Mobile phones with camera and video functionality
- Smart phones with e-mail, messaging and internet access

Roles and responsibilities
Within the school all members of staff and students are responsible for e-safety, responsibilities for each group include:

Governors:

- Approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor.

The role of the E-Safety Governor will:

- regularly meet with the ICT Manager/Designated Senior Person
- reporting to relevant Governors

Head teacher and Senior Leaders:

- Ensure the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the ICT Manager.
- Be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – Appendix 1).
- Be responsible for ensuring that the ICT Manager and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- Ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

ICT Manager / Curriculum Leader:

- Ensure that the best technological solutions are in place to ensure e-safety as much as possible whilst still enabling students to use the internet effectively in their learning.
- Ensure that all information captured using these systems is secure, accessible to the appropriate members of staff, and stored in a robust manner. In addition securing and preserving evidence of any e-safety breach.
- Checks and audits all systems to ensure that no inappropriate data is stored or is accessible.

- Works with the Curriculum Leader to create, review and advise on e-safety and acceptable use policies.
- Leads the development of the e-safety education programme for students and staff.
- Manages a parental awareness programme for e-safety.
- Deals with e-safety breaches from reporting through to resolution in conjunction with the ICT support team.
- Works with outside agencies including the police where appropriate.
- Maintains a log of all e-safety issues.
- Monitors the technology systems which track student internet use to detect e-safety breaches.
- Assists in the resolution of e-safety issues with other members of staff.

All Staff:

- Have a clear understanding of e-safety issues and the required actions from e-safety training sessions.
- Reporting any e-safety issues to the ICT Manager as soon as the issue is detected.

Teaching Staff:

- Educating students on e-safety through specific e-safety training sessions and re-enforcing this training in the day to day use of ICT in the classroom.

Pupils:

- Participating in and gaining an understanding of e-safety issues and the safe responses from e-safety training sessions.
- Reporting any e-safety issue to the teacher, team leader or parent.
- Take responsibility for their own actions using the internet and communications technologies.

The school shall:-

- Use the filtering system put in place by the LA
- Supervise children's internet use
- Encourage children to report accidental access to inappropriate materials
- Provide class rather than individual e-mail accounts for pupils so that an adult can monitor incoming and outgoing mail.
- Teach children the importance of keeping usernames and passwords private.
- Ensure that log-in policies preclude children from downloading innappropriate internet based material.
- Provide appropriate opportunities within the curriculum to teach internet safety including Web 2 technologies.

*The school recognises that it is impossible to completely remove the risk pupils inadvertently accessing unsuitable materials via the school system. To minimize this risk, the school will constantly supervise pupils and take all reasonable precautions that only appropriate material is access*ed*. Therefore, neither the school nor the LA can accept liability for any material that is accessed or any consequences thereof.*

Keeping children with SEN safe
Through ICT we ensure that the school meets the needs of all children, taking account of gender, ethnicity, culture, religion, language, age, ability, disability and social circumstances. It is important that in this school we meet the diverse needs of pupils to

ensure inclusion for all and that all pupils are prepared for full participation in a multi-ethnic society.
Our SEN co-ordinator and individual teachers must ensure all children have equal access to succeed in this subject.

- The ICT Manager provides a list of age appropriate websites which children may access in school or at home
- During research activities SEN pupils will be supervised, and where necessary supported to minimise risk and keep them safe.

E-safety in the curriculum

- ICT and online resources are increasingly used across the curriculum. We believe it is essential for E-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for opportunities to promote E-Safety.
- Educating pupils on the dangers of technologies that maybe encountered outside school is undertaken informally when opportunities arise and as part of the ICT curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modeling and activities.
- Pupils are aware of the impact of Cyber-bullying and know how to seek help if they are affected by any form of online bullying (see Anti-Bullying Policy). Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Childline or CEOP report abuse button.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.
- The school uses an approved filtering system at all times. Only teachers laptops can access websites such as YouTube.

The misuse of technology

Whenever a student or staff member misuses technology, the final decision on the level of sanction will be at the discretion of the Head teacher/School Leader and or Governing Body.

Pupils:

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites
- Accidentally accessing offensive material and not notifying a member of staff of it
- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Staff:

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network
- Serious misuse of, or deliberate damage to, any school computer hardware or software;

- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school into disrepute.
- The use of school systems for personal financial gain, gambling, political purposes, advertising, accessing inappropriate materials e.g. pornographic, discriminatory or offensive material is forbidden.

Child Pornography:

In the case of child pornography being found, the member of staff will be immediately suspended and the school disciplinary procedures implemented.

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.
- Where appropriate, involve external agencies as part of these investigations.

How will staff and students be informed of these procedures?

- All staff are required to sign the school's e-safety Policy acceptance form;
- Pupils will be instructed about responsible and acceptable use and given strategies to develop 'safe behaviours'. Pupils are required to sign an age appropriate e-safety / acceptable use form (Home-School agreement)
- The school's e-safety policy will be made available to parents who are required to sign an acceptance form when their child starts at the school. (Home school agreement)

Parental Involvement
Many pupils will also have access to ICT and the internet at home, often without some of the safeguards that are present within the school environment. Therefore parents must often be extra vigilant about their child's e-safety at home.

One of the goals of the school is to support parent's role in providing an e-safe environment for their children to work in outside the school.

The school will do this in several ways;

- Run training sessions and workshops on e-safety.
- Publish e-safety information via the school website.

Using Images And Video Safely On Websites

- Parental permission is required before a child's photograph is used on the internet.
- Where possible group photos rather than photos of individual children will be used.
- The propriety of photographs and video will be carefully considered before use.
- We will not use the names of individuals in a photograph to reduce the risk of inappropriate, unsolicited attention from people outside school.

- If the pupil is named, we will not use their photograph; if a photograph is used, we will not name the pupil.
- All image files will be appropriately named – we will not use pupils' names in image file names or ALT tags if published on the web. This will avoid names being ascertained from source code.

The management of email

Pupils:

- 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.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations 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.
- Misuse of email e.g. sending offensive emails will result in sanctions as stated in Misuse of Technology

Staff:

- Staff may only use approved e-mail accounts on the school system; school email addresses should always be used for school business.
- Staff must immediately tell the Head teacher/School Leader/ICT Manager if they receive offensive e-mail.
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- Misuse of email e.g. sending offensive emails will result in sanctions as stated in Misuse of Technology

Passwords and password security

- Staff are provided with an individual network/ Email username and password.
- Pupils/students are not allowed to deliberately access on-line materials or files which are the property of other users.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS systems including ensuring that passwords are not shared. **Individual staff users must also make sure that open workstations are not left unattended and are locked or logged off.**

The use of mobile technology

Children:

- The school forbids the use of personal cameras, mobile telephones and recording devices by pupils whilst in school or on the school grounds.
- All pupils are required to store mobile phones in the school office upon entering the school. Children will need to collect their mobile phones at the end of each school day.
- Pupils must not take mobile phone devices on any school trips or to any outside activities where they are representing the school.
- Immediate action will be taken by the Head teacher / School Leader of any pupil is found with their mobile device during school hours.

Staff:

- The school forbids the use of personal cameras, mobile telephones and recording devices by staff members, students and volunteers whilst on duty.
- All staff, students and volunteers who are working with children are required to switch off any mobile phones and recording devices and store them in a lockable cupboard during working hours.
- Staff members and volunteers may access their personal devices whilst off duty, for example during lunch breaks. Designated areas for this will be the office and staff room.
- Staff using personal mobile devices during session times will be subject to school disciplinary procedures
- Personal mobile devices may be taken during off-site visits and trips, but must be turned off when working with the children.
- 2 dedicated school mobile phones will be kept in the office, to be taken on off site visits. This will be left on in case of emergency, and in the possession of the senior teacher on the trip. This will not have image capability.
- A dedicated school mobile phone will be in the possession of the caretaker. This will not have image capability.
- Children will only be photographed or recorded by the use of a camera/recording device that has been agreed by the head teacher or setting manager.
- Children will only be photographed or recorded if parental consent has been obtained or for in-school assessment procedures

The use of webcams

We do not use publicly accessible webcams in school. Webcams in school are only ever used for specific learning purposes, i.e. monitoring hens eggs. Misuse of the webcam by any member of the school community will result in sanctions (as listed under Misuse of Technology).

- Peripheral webcams will be set up/monitored by the ICT Manager or members of staff.

The use of video conferencing (Not currently applicable at Corpus Christi Catholic Primary School)

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- External IP addresses should not be made available to other sites.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing should be supervised appropriately for the pupils' age.

Monitoring and evaluation

- The ICT Manager will actively monitor the students ICT activity using a monitoring system which can flag potential e-safety issues.
- The ICT Manager will periodically review internet access logs to track any websites which could potentially present an e-safety issue and use the information to look at ways of improving the student's e-safety.

Reviewed September 2015 by L.Cain (School Leader), Lesley O'Doherty (ICT Manager), Denise O'Flynn (SENCo)

APPENDIX 1

How to report an e-Safety incident