Catholic School

St Peter's

GUILDFORD

E-safety Policy

Entity Responsible – SLT
Last review: Summer 2016
Next Review: Summer 2017

This e-safety policy forms part of the School Development Plan and should be read in conjunction with other policies including Behaviour and child protection.

The school will appoint an E-safety Coordinator with suitable skills and experience including an appreciation of the issues arising from bullying and Child protection. This is not a technical role and can be undertaken by any suitable member of staff.

Our E-safety Policy has been written by the school based on best practice and government guidance.

The policy and its use will be reviewed on an annual basis by the School Leadership Team.

E-Safety policy

E-safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for **behaviour, safeguarding and data protection and the Acceptable Use Policies (AUP)**

Using this policy

- The school will form an e-safety committee and will appoint an e-safety co-ordinator.
- Our e-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by school leadership team.
- The e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / student

Managing access and security

The school will provide managed internet access to its staff and students in order to help students to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by secure personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by school leadership team and have clear procedures for reporting issues.
- The school will ensure that access to the internet via school equipment for anyone not employed by the school is filtered and monitored.

Internet Use
The school will provide an age-appropriate e-safety curriculum that teaches students how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Students will be advised not to give out personal details or information which may identify them or their location.

All communication between staff and students or families will take place using school equipment or appropriate software.

E-mail

- Students and staff may only use approved e-mail accounts on the school IT systems.
- Staff to student email communication must only take place via a school email address or appropriate software.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Published content eg school web site, school social media accounts

- The contact details will be the school address, email and telephone number. Staff or students personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Students images and work

- Written permission will be obtained from parents or carers before photographs or names of students are published on the school web site or any school run social media as set out in Surrey Safeguarding Children Board Guidance on using images of children.

Use of social media including the school learning platform

- The school will control access to social networking sites, and consider how to educate students in their safe use. This control may not mean blocking every site; it may mean monitoring and educating students in their use.
- Use of video services such as Skype, Google Hangouts and Facetime will be monitored by staff. Students must ask permission from a member of staff before making or answering a video call.
- Staff and students should use ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community.

Use of personal devices

- Personal equipment may be used by staff and/or students to access the school IT systems provided their use complies with the e-safety policy and the relevant AUP.
- Staff must not store images of students or student personal data on personal devices.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data

- The school has a separate Data Protection Policy. The AUP covers the treatment of student and staff personal data on and off site and remote access to school systems. There is a separate consent form for the use of Biometric data.

Policy Decisions
Authorising access

- All staff, governors and visitors must read and sign the 'Staff Governors and Visitors AUP' before accessing the school IT systems.
- The school will maintain a current record of all staff and students who are granted access to school IT systems.
- Students must apply for internet access individually by agreeing to comply with the student AUP.
- Parents will be asked to sign the ICT user agreement in their son/daughter's journal to allow use of technology.

Assessing risks

- 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. Neither the school nor SCC can accept liability for the material accessed, or any consequences of internet access.

Handling e-safety complaints

- Complaints of internet misuse will be dealt according to the school behaviour policy.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents will be informed of consequences and sanctions for students misusing the internet and this will be in line with the schools' behavior policy.

Community use of the internet

- Members of the community and other organisations using the school internet connection will have signed a guest AUP so it is expected that their use will be in accordance with the school e-safety policy.

Protocol to be used for any allegations of "Youth Produced Sexual Imagery"
(previously referred to as Sexting)

- Remember youth refers to any young person under the age of 18, if older people are involved then it is Child abuse and must be reported to the MASH – Multi Agency Safeguarding Hub.

- Incident takes place or any well founded allegation:
  Refer to DSL – GGO
  GGO will review incident with HoY, MTW, (+ any other teacher involved eg mentor etc) using Brook Traffic Light Toolkit
  DSL to interview young person(s)
  DSL to inform parents – keep conversations open provide parents with information and resources from NSPCC
  If young person at risk of harm DSL to refer to MASH or Police

- First member of staff involved must confiscate the device, there is no need to look at image, do not take copies, do not forward to anyone. Keep device locked up until decisions have been made.

- If there is no Police involvement – delete image and return device.
  If Police are involved – retain device and hand to Police.

- Generally if the issue occurs during the school day, during an off-site activity/trip or during travel to/from school, then school will investigate.
  If the issue occurs outside of school, then the school will provide support.

- If the issue occurs outside of school, but involves any content recorded during school related activity, then the school investigate.
  Any issue aimed at staff, the school, or the reputation of the school will be investigated regardless of when it occurs.

- Please refer to the Behaviour Policy for sanctions.

Communication of the Policy
To students

- Students need to agree to comply with the student AUP in order to gain access to the school IT systems and to the internet
- Students will be reminded about the contents of the AUP as part of their e-safety education

To staff

- All staff will be shown where to access the e-safety policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP in order to gain access to the school IT systems and to the internet
- All staff will receive e-safety training on an regular basis

To parents

- The school will ask all new parents to sign the ICT user agreement when their child starts with the school.
- Parents will be offered e-safety training annually