CORPUS CHRISTI
CATHOLIC SCHOOL

E-safety Policy

2019

Date	Review Date	Coordinator	Nominated Governor
16.09.19	September 2020	R Kriechbaum	M Sawyer

Corpus Christi E-safety Policy

This policy is a living document, subject to annual review but also amended where necessary during the year in response to developments in the school and local area.

Online-safety risks are usually categorised as one of the three Cs: Content, Contact or Conduct. These three areas remain a helpful way to understand the risks and potential school response, whether technological or educational. They do not stand in isolation, however, and it is important to understand the interplay between all three.

Rationale

The Internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration systems. Internet use is an essential element in 21st century life; therefore access to the Internet is an entitlement for pupils who must be taught to show a responsible and mature approach to its use. Our school has a duty to provide pupils with a high quality experience of the Internet.

Many of the risks associated with the 'on-line' world also reflect situations in the 'off-line' world and it is essential that this e-safety policy is used in conjunction with other school policies such as the behaviour, anti-bullying and child protection policies.

We also have a duty to safeguard children, young people and families from violent extremism. We are aware that there are extremists groups within our country who wish to radicalise vulnerable children and to involve them in terrorism or in activity in support of terrorism. School personnel must be aware of the increased risk of online radicalisation, and alert to changes in pupil's behaviour. Any concerns will be reported to the Designated Safeguarding Lead.

Aims and Objectives

- To provide pupils with quality Internet access as part of their learning experience across all curricular areas.
- To provide clear advice and guidance in order to ensure that all Internet users are aware of the risks and the benefits of using the Internet.
- To evaluate Internet information and to take care of their own safety and security.
- To raise educational standards and promote pupil achievement.
- To protect children from the risk of radicalisation and extremism.
- To ensure compliance with all relevant legislation connected to this policy.

Computing has an all en-compassing role within the lives of children and adults, both within school and the wider community. Current and emerging technologies used in school and, perhaps more importantly, outside of school by children can include:

- The Internet
- The World Wide Web
- e-mail
- Instant messaging - often using web cams, for example Skype, Snapchat, Whatsapp or Instagram, Musicli
- Blogs
- Podcasts

- Social networking sites
- Video broadcasting sites
- Chat rooms
- Online gaming sites
- Music download sites
- Use of mobile phones with camera and video facilities
- Mobile technology that is 'Internet Ready'
- Games consoles that are 'Internet Ready'
- Smart phones
- Tablet technology, such as iPads

The use of such technology greatly enhances communication and the sharing of information. At Corpus Christi School, pupils and staff are to be encouraged to use them in a positive and responsible way. However, their use can put young people at risk within and outside of school. Some of these dangers include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the Internet
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / Internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

It is the duty of the school to ensure that every child in their care is safe and the same principles should apply to the 'virtual' or 'digital' world as would be applied to the school's physical building.

The policy document has been drawn up to protect all parties - the pupils, the staff and the school and aims to provide clear advice and guidance on how to minimise risk.

Corpus Christi is very aware of the vulnerability of our SEND pupils with regards to e-safety. As such, a specific SEND acceptable use agreement is used for pupils who may require it. The home school-partnership with these families is especially vital to ensure that the risks posed for these pupils are minimised as much as possible. Parents of these children are actively encourages to attend parent e-safety workshops. Risk management and at home strategies should also be discussed in annual reviews for those pupils concerned.

Roles and Responsibilities

This policy applies to all pupils, parents and carers, teaching and support staff, governors, students, part-time staff, mid-day supervisors, music tutors, sports coaches, volunteers and visitors. This list is not to be considered exhaustive.

The role of the Designated Person/s for Child Protection

- To attend training in e-safety issues and be aware of the potential for serious child protection issues which arise from:

  - ✓ Sharing of personal data
  - ✓ Access to illegal / inappropriate materials
  - ✓ Inappropriate on-line contact with adults / strangers
  - ✓ Potential of actual incidents of grooming
  - ✓ Cyber-bullying
- To provide support and advice to staff as regards potential online-safety issues.
- To liaise with the Computing subject leader and other staff in regards to the implementation and monitoring of the e-safety programme of work.
- To update the Head Teacher(s) and Governors of any e-safety issues that need attention.

The Role of Teaching and Support Staff

- To have an up-to-date awareness of e-safety matters and of the current school policy and practices related to e-safety.
- To report any suspected misuse or problem to the designated person/s for child protection for investigation / action / sanction.
- To ensure any digital communications with pupils are on a professional level and only carried out using the official school systems.
- To ensure personal information, including telephone contact details, are not provided to pupils.
- To carry out the school's e-safety programme of work and embed it in everyday practice in all aspects of the curriculum.
- To ensure pupils understand and follow the online-safety rules. A copy should be easily accessible to the pupils; for example displayed in the classroom and computing suite. The copies available should be appropriate for the age and understanding of the pupils.
- To ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- To monitor computing activity in lessons and extra-curricular / extended school activities as appropriate.
- To be aware of online-safety issues related to the use of mobile phones, cameras and hand held devices which should not be within the children's possession in school.
- To ensure that in lessons where Internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with unsuitable material that is found in Internet searches.
- To understand the contents of this policy and other e-safety related policies and to sign the Staff E-Safety Acceptable Use Form (see Appendix 1).
- Many of the new online safety risks are mentioned in KCSIE 2019, e.g. fake news, upskirting and sticky design. All staff must read this supporting document so that they are aware of these risks.
- To attend online safety training.

The Role of Pupils

- To abide by the school's rules for safe Internet use.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- To abide by the school's policy as regards to the use of mobile phones, cameras and other digital devices.
- To understand the importance of adopting good online-safety practices outside of school.
- To understand and abide by the school's anti-bullying policy.
- To avoid plagiarism and uphold copyright regulations.

The Role of Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use internet and their mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, e-safety campaigns and other literature. Parents and carers should understand the contents of this policy.

Curriculum

The school uses online-safety curriculum lessons as part of the 'Switched on Computing' scheme of work'. Computing lessons and school assemblies will be dedicated to teaching pupils about online-safety and how to deal with any issues which might arise. The teaching of online-safety is embedded across the curriculum, especially when technology is used.

Use of digital and video images

Examples of how digital photography and video may be used within the school include:

- Pupils being photographed by the class teacher, teaching assistant or other pupils as part of a learning activity e.g. photographing pupils at work which may be displayed or recorded in exercise books, allowing the pupils to see their work and make improvements.
- A pupil's image for presentation purposes around the school e.g. in school displays, on School Council/Green Team boards, to promote different school activities.
- A pupil's image being used for promotional literature such as the school prospectus, website or Twitter account.
- On rare occasions, a pupil's image may appear in the media if a newspaper photographer or television film crew attend a school event.

NOTE: If a circumstance arose where the school wanted to link a pupil's image to their name e.g. if the pupil won a national competition and wanted to be named as a result of this, parental permission would be sought separately on these occasions.

The following safeguarding principles are followed with specific regard to the use of digital and video images:

- The school will gain parental/carer permission for the use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school. As of 2018 and due to the recent changes in GDPR laws, permission will be gained from parents and carers again to use photographs involving their child.
- Only images of pupils in suitable dress are used.
- Parents volunteering on class trips are not allowed to take photographs or videos on their personal equipment.
- Any digital videos or images of pupils should only be saved on the school 'shared' 'media' and 'staff' drives on the network.
- The school does not identify pupils in online photographic materials or include the full names of pupils in any materials published by the school.
- All staff sign the school's 'Acceptable Use Policy' and this includes a clause on the use of mobile phones and personal equipment for taking pictures of pupils.
- The school blocks/filters access to social networking sites/blogs unless there is a specific approved educational purpose.
- Pupils are advised to be very careful about placing any personal photos on any social online network space. They are taught to understand the need to maintain privacy settings so as to not make public any personal information.

- Pupils are taught that they should not post images or videos of others without their permission. They are taught about the risks associated with providing information that reveals the identity of others and their location such as address or school name. Pupils are taught about the need to keep their data secure and what to do if they are subject to bullying and abuse online or offline.
- Explicit permission must be gained from parents to use their child's images on school material, the website or twitter.

Website

- The headteacher(s) takes overall editorial responsibility to ensure that the website content is accurate and well presented.
- Uploading of information is restricted to approved website editors.
- The school website complies with the school guidelines for publications.
- Most material on the website will be the school's own work; where others work is published or linked to, the school will credit the sources used and clearly identify the author.
- The point of contact on the website is the school address, telephone number and office email address: office@corpuschristi.lambeth.sch.uk
- Photographs published on the website will not include any names.
- Pupil names will not be used when saving images or in the tags when publishing to the school website.

Twitter

The school has its own Twitter account which is used to communicate information and pictures which are of interest to parents, the local community and a wider audience of followers. The following safeguarding principles have been put in place:

- Permission to 'upload' to Twitter will be restricted to those authorised by the Headteacher(s). At any one time, this should be no more than two or three members of staff in order to maintain control of Twitter content.
- Any other member of staff who would like to upload to Twitter will forward their photo or video to the designated member of staff who will check that the image is suitable before uploading.
- The content of all photos and videos that are uploaded will follow the same guidelines as set out in this document.
- The designated members of staff responsible for the Twitter account will regularly check any comments that are posted and check the suitability of those 'following' the school's account. They will take the necessary steps to delete/block any comments or followers deemed inappropriate.

E-mail

- Pupils may only use approved e-mail accounts on the school system provided by the LGfL.
- Pupils will be encouraged to tell a member of staff if they receive an offensive e-mail.
- Pupils will be taught to not reveal personal information about themselves or others in e-mail communication, or arrange to meet anyone with parental permission and agreement.
- Access to personal, external e-mail accounts may not always be possible if certain e-mail sites are blocked.

- School e-mail messages sent to organisations should be written carefully and checked before sending, in the same way that a letter written on school headed paper would be.
- Staff should use the school e-mail system for official school business only. All staff should be made aware that e-mail messages are subject to 'freedom of information' requests in the same way as other information is within the school setting.

Filtering

The filtering of Internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system can not, however, provide a 100% guarantee that it will do so. It is important that the school's filtering policy is regularly monitored and updated and able to manage the associated risks.
The school will continue to subscribe to the filtering service provided by the London Grid for Learning (LGfL) and their appointed service provider (currently Virgin Broadband). The school will apply the suggested website filters; but will maintain the ability to block / un-block certain sites when any reasonable request is made and the relevant website is checked for suitability. The members of staff able to make changes to the school's filtering policies are:

- The headteacher(s)
- The Computing Co-ordinator
- The School Business Manager
- Appointed ICT technicians

Communication of Policies

Pupils

- Rules for Internet access will be posted in the main computer suite.
- Pupils will be made aware that Internet use will be monitored
- Pupils that are old enough to access the Internet independently will be asked to sign an age appropriate 'Acceptable Use Policy'.

Staff

- All staff will be given a copy of the school's online-safety policy and will have an opportunity to discuss its content.
- All staff will be made aware that the use of the Internet in school should be for educational purposes only and that Internet traffic can be monitored and traced back to the individual user. Discretion and professional conduct is essential.
- All staff will be asked to sign an 'Acceptable Use Policy'
- All staff will be required to attend any online-safety training deemed necessary by the school leadership team or online-safety co-ordinator.

Parents / Carers

- Parents' attention will be drawn to the school's online-safety policy through the appropriate means.
- Parents will be encouraged to discuss the 'Acceptable Use Policy' with their child(ren) when appropriate
- Parents will be encouraged to discuss with the school any concerns / questions they have with regard to the safety of their child(ren) whilst on-line.
- Parents will be invited to regular online safety meetings to discuss any concerns they may have, as well as to educate themselves about how to keep their young people safe online.

Conclusion

As with all other risks, it is impossible to eliminate them completely. It is therefore essential, through good educational provision to build pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with them as and when they present themselves.

This e-safety policy will enable the school to demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably expected of them to manage and reduce these risks.

Date: September 2019	**Review:** September 2020