St John Evangelist Catholic Primary School

E-SAFETY POLICY

Mission Statement: To love, to learn with God in our hearts

Policy revised: February 2024 Review Date: February 2025

Today's pupils are growing up in an increasingly complex world, living their lives seamlessly on and offline. This presents many positive and exciting opportunities, but also challenges and risks.

We want schools to equip their pupils with the knowledge needed to make the best use of the internet and technology in a safe, considered and respectful way, so they are able to reap the benefits of the online world. DfES 2019

Keeping Children Safe In Education tells us that 'It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

Whole school approach to the safe use of ICT

Creating a safe ICT learning environment includes four main elements at this school:

- An effective range of technological tools;
  Policies and procedures, with clear roles and responsibilities;
- A comprehensive e-Safety education programme for pupils and staff;
- Support for parents on how to identify and use the internet safely at home with and for their children to support their learning.

Risks and Issues

The following are the range of technologies children/young people and staff/volunteers use positively but which can also put them at risk:

- Internet

- E-mail
- Instant messaging
- Blogs
- Podcasts
- Social networking sites
- Chat rooms
- Gaming Sites
- Mobile phones with camera and video functionality
- Mobile technology (eg games consoles) that are internet ready and include webcams E-smart phones with e-mail, web functionality, camera and video functionality and secure text network

Roles and Responsibilities
e-Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school. The head teacher ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to the ICT lead who is supported by the designated safeguarding lead. Governors need to have an overview understanding of e-Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. Central to this is fostering' No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff should be familiar with the schools' Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of school network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones, iPads, laptops and digital cameras;
- Publication of pupil information/photographs and use of website;
- eBullying / Cyber bullying procedures;
- Their role in providing e-Safety education for pupils.

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 buildings. For information regarding remote learning, please see the school's remote learning policy.

School Safeguarding Actions
The school, through staff, networks and promotions of appropriate uses policies, ensures the following:

- Supervises pupils' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older pupils have more flexible access;
- We use the London LGfL / Virgin Media filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Staff are expected to preview all sites before use [where not previously viewed and cached] or only use sites accessed from managed 'safe' environments such as the Learning Platform;

- Plans the curriculum context for internet use to match pupils' ability, using child-friendly search engines where more open internet searching is required;
- All Google image searches are tested, where possible by staff before use.
- Informs users that internet use is monitored (visiting the history icon shows usage)
- Informs staff and students that that they must report any failure of the filtering systems directly to the ICT Leader.
- Blocks all chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Ensure that permission is granted to publish anything on the school's social media site(s), website or app, whilst also ensuring the data published is accurate and correct;
- Only uses Google Classroom or LGFL for pupil's own online creative areas such as Google Docs, Google Drive, JiT, J2e and creative toolkit;
- Only uses approved Blogging or discussion sites, such as on the LGfL / approved Learning Platform and blocks others.
- Only uses approved or checked web cam sites;
- Has blocked pupil access to music download or shopping sites – except those approved for educational purposes such as LGfL's Audio Network;
- Requires pupils (and their parent/carer) from Key Stage 1 and 2, to individually sign an e-safety / acceptable use agreement form which is fully explained and used as part of the teaching programme;
- Requires all staff to sign an Acceptable Use Agreement form and keeps a copy on file;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record, e.g. on CPOMs, of any bullying or inappropriate behaviour for as long as is reasonable in-line with the school behaviour management system;
- Ensures parents provide consent for pupils to use the internet, as well as other ICT technologies, as part of the Acceptable Use Agreement form at time of their daughter's / son's entry to the school;
- Immediately refers any material we suspect is illegal to the appropriate authorities – LA / Police.

How will complaints regarding e-Safety be handled?

Staff and pupils are given information about infringements in use and possible sanctions. Our ICT Leader acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Head teacher.

Complaints of cyber bullying both at home and in school are dealt with in accordance with our Anti-Bullying Policy/ Behaviour Policy. Complaints related to child protection and safeguarding are dealt with in accordance with school / LA child protection and safeguarding procedures and must be discussed with the DSL and recorded according to the school procedure.

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school leadership.

The school's Acceptable Use policy is explained to staff / Governors, pupils and parents, with all signing acceptance / agreement forms appropriate to their age and role. The school makes it clear possible sanctions for infringements.

Useful Websites

- Islington Safeguarding Children Board – e-safety page http://www.islingtonscb.org.uk/key-practice- guidance/Pages/E-safety.aspx
- Internet Watch Foundation http://www.iwf.org.uk/
- BBC Learning zone www.bbc.co.uk/learningzone/clips/5594.flv http://ceop.police.uk/
- Childnet International http://www.childnet-int.org
- Cyberbullying www.digizen.org
- Cybermentors https://cybermentors.org.uk/ http://www.getsafeonline.org/