St Mary's Catholic School
E-safety policy

This policy aims to help individuals understand their roles and responsibilities in ensuring the safe and acceptable handling/use of information technologies.

Applicable to all users of technology and connected systems:
Unlawful/inappropriate material must not be viewed/stored/distributed on any school system. This can include material which is in violation of any law/regulation or which can be considered by any reasonable person in its context to;

- be defamatory
- be violent
- be offensive
- be abusive
- be indecent or obscene
- be discriminatory
- incite hatred
- constitute bullying and/or harassment
- breach anyone's confidence, privacy, trade secrets or copyright

General guidelines for staff

- If someone has stated that they do not wish to receive emails from you then you must refrain from sending further e-mails to them. You must not use an organisation's email systems for 'spamming' purposes (the use of email to send unwanted/junk/advertising content to multiple recipients).
- Particular care should be taken whenever you choose to use your own personal technologies in a work environment and ensure that other people, including children, are not able to see personal contents which you would deem private or sensitive.
- You must ensure that your work/school computer account is not misused so you should not share your username or password with anyone. All Internet and network use of systems may be subject to monitoring by school and this may be traced back to you. Everyone is responsible for ensuring information systems are secure, safe and used to benefit all. You should be aware that disciplinary/civil/criminal action might arise if any user is found to be deliberately accessing material described above. Similarly, unauthorised or deliberate illegal access to or use of data, systems or networks is prohibited and may also result in disciplinary/civil/criminal action.

Information system security

- The School's ICT system capacity and security will be reviewed.
- Virus protection is installed and updated regularly.
- Security strategies will be discussed with the LA and implemented to ensure best practice is maintained.
- Unapproved system programs, utilities and executable files will not be allowed in students' work areas or attached to e-mail.

E-mail

- Students will be encouraged to use approved e-mail accounts on the school system, the use of personal web mail accounts such as Hotmail may be blocked as appropriate.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be in a professional manner.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details on the Web site will be the school address, e-mail 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

- Photographs that include students will be selected with children's safety in mind.

- Students' full names will not be used anywhere on the Web site without express permission.
- Written permission from parents will be obtained before photographs of students and/or full names are published on the school Web site or any other medium.
- When publishing students' work, staff must take care to ensure that no personal information is revealed in the work that can be connected to a student.

Social networking and personal publishing

- School will block/filter access to social networking sites wherever possible.
- Newsgroups will be blocked, where possible, if they contain inappropriate material.
- Students will be advised never to give out personal details of any kind which may identify them or their location.
- Students will be advised not place inappropriate photos or personal details on any social network space and made aware of the security implications of this.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications.

Managing filtering

- While the school makes every effort to protect students from unsuitable materials, due to the international scale and connected nature of Internet content, it is impossible to guarantee that unsuitable material will never appear on a school computer. Filtering is carried out by both the LA and the school.
- The school will work in partnership with the LA, DfE and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover an unsuitable site, it must be reported to the ICT Manager.
- Regular checks are made to ensure that the filtering methods selected are appropriate and reasonable.
- The use of "proxy sites" to bypass school or LA filters is prohibited and the school will endeavour to block these.

Managing videoconferencing and filming/photography

- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Videoconferencing will be appropriately supervised for the students' age.
- Parents and carers should agree for their children to take part in videoconferences, filming or photography, in the annual data collection sheet at the start of the academic year.
- Personal recording equipment, cameras and mobile phones must not be used in school without permission from the class teacher.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones of students must be switched off and out of sight at all times in school.
- Staff should not provide their mobile phone number to parents or students. A school contact mobile number is available for all visits.
- In exceptional circumstances, such as school trips, staff can be provided with a mobile phone for use.

Assessing risks

- **Protecting personal data** will be recorded, processed, made available according to Data Protection Act 1998.
- 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 NCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Policy review date	**By whom**	**Approved** *(insert date)*
October 2014	FGB meeting	01/10/14

December 2015	FGB- Academy Directors	10/12/15
September 2019	FGB- Academy Directors	20/09/19