# ST JOSEPH'S CATHOLIC HIGH SCHOOL

# ICT SAFETY AND E-SAFETY
# Part 1 – Use of Internet

**Date of Review October 2018**
**Due for Review October 2020**

The purpose of this document is to update our existing policies and practices and consolidate them into one document for ease of use and accessibility. The key documents that this document has been written include SSCB's *Guidance on The use of Email and Text messaging for professionals*, *Guidance using Images of Children: Photographs, Videos, Websites and Webcams* , OFSTED's *The Safe Use of New Technologies* (2010) and *School Evaluation: A response to the Byron Review* (2008). This policy reflects the guidance in those documents and seeks to draw its fundamental principles on safety into our school community. This document consists of 4 parts.

## Part 1
## Safe use of the Internet

**Aim of this policy:**

- To promote the enhancement of learning and teaching in an atmosphere where all staff adopt safe practices in the use of the internet and in the teaching of internet use to children.
- To educate children to be responsible and informed internet users.
- To inform and support parents in keeping their children safe on the internet at home.

Our policy will ensure that we will:

- Audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies. This will be renewed annually with the Governors subcommittee on Safeguarding. E-safety training should become included in training for child protection and Induction.
- Work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at school. For example: this has hitherto been achieved by a combination of external expert speakers and parent information evenings for each year group on an annual basis where the issue of internet safety has been be directly addressed.
- Use pupils' and families' views often to develop e-safety strategies. This will be achieved through systems such as the student voice and parent voice.
- Work towards a managed internet access system to help pupils understand how to manage risk; to provide them with richer learning experiences; and to bridge the gap between systems at school and the more open systems outside school.
- Provide an age-related, comprehensive curriculum for e-safety which enables pupils to become safe and responsible users of new technologies. This is achieved throughout the school curriculum from year 7-11 and on enrichment days and in assemblies in years 1213. This covers:

    1) using social networking sites and websites
    2) dealing with cyber-bullying.
    3) managing mobile phones, email and instant messaging
    4) sharing personal images
    5) using data and protecting passwords 6) avoiding pornography.

- Work with their partners and other providers to ensure that pupils who receive part of their education away from school are e-safe. Where concern is raised the first point of contact should be the designated CPLO.
- Systematically review and develop their e-safety procedures, including training, to ensure that they have a positive impact on pupils' knowledge and understanding. This is the responsibility for the Leadership Team of the school and the Governors subcommittee on Safeguarding.

As we are moving towards a situation where ICT is an integrated way of learning across the whole school it is of high importance that all teachers are alert to and take responsibility for the safety of the students when using the internet when under their care in the learning environment. Teachers must ensure that they:

- Recognise and manage the potential risks associated with online activities
- Recognise and draw to the students' attention when pressures from others in the online environment might threaten their personal safety.
- Outline clear expectations to all students about online behaviour and deal effectively with misuse of the online activity.
- Teachers should outline to students the importance of;
- not to reveal personal details when using the internet
- not to give their password to other people
- to report any suspicious sites
- to ensure that any mobile devices that they might wish to attach to school equipment were free of viruses
- not to make defamatory comments about others online.
- consequences of breaching the regulations, with the normal school disciplinary sanctions which may depending on the nature of the breach may include contacting parents directly together with referring the breach to the Head of Year, a member of the Leadership Team or the CPLO as appropriate and which may include the possibility of banning pupils from using the school's computer system for a defined period.

**Staff should be aware that communicating with students via social networking media is prohibited. In certain controlled circumstances learning based activities may be conducted using social networking media or email but these should always occur through school based accounts and focus on learning and teaching activities. Staff should not under any other circumstances make contact or respond to students attempts to make contact via text, email or social networking media.**