E-SAFETY

POLICY AND PROCEDURE

Written by:	Director of Technical Support
Date:	August 2018
Review Date:	August 2019
Person responsible for review:	Director of Technical Support

AMDG

E-Safety Policy

Introduction

The term 'e-safety' is used to encompass the safe use of all technologies in order to protect children, young people and adults from potential and known risks.

It is the duty of Stonyhurst College and St Mary's Hall to ensure that children and young people are protected as much as possible from potential harm both within and beyond the school, including in boarding areas.

We aim:

- To promote awareness amongst our pupils about the dangers they (and all users) can face on line
- To give our pupils (and other users) advice about how to protect themselves and others, what to do if they should encounter such dangers, and whom to tell
- To promote understanding of the dangers of sexting or of posting inappropriate photographs online
- To do all we can to protect the Stonyhurst network through the use up to date technology, software and systems, and by doing so to protect the pupils and staff who access the internet through the network
- To encourage pupils to behave responsibly and safely, and to protect themselves from danger, when they use the internet through potentially unfiltered devices and networks (such as 3G or 4G services on their own smart phones or tablets)

Roles and Responsibilities

It is the overall responsibility of the **Governors** to have an overview of E-Safety as one element of the wider remit of safeguarding across the campus.

It is the responsibility of the **Headmaster** and **DSL** to ensure that any untoward incident relating to e-safety is dealt with appropriately, according to Stonyhurst's published procedures, in particular the Safeguarding policy, and that appropriate action is taken.

It is the responsibility of the **Director of Technical Support** to:

- ensure that appropriate firewalls and filters are in place, as well as anti-virus and anti-spyware software
- promote the safe use of wireless technology
- issue guidance on the safe and contstructive use of personal devices both in and out of the classroom
- to ensure that all users are familiar with, and agree to, the Stonyhurst Acceptable Use Policy

It is the joint responsibility of the **Magis co-ordinator** and the **ICT teachers** at St Mary's Hall and the College to ensure that up-to-date, age-appropriate E-Safety education is provided within the curriculum to pupils as they progress through the two schools. Details of the content and delivery of of lessons in E-Safety, which include promotion of the awareness of risks associated with online radicalisation and extremism (with reference to the Prevent duty) are available in the College Magis PSHE Programme (pages 10, 14, 15 and elsewhere) and appendices; and College and SMH Schemes of Work for ICT. Topics relating to E-Safety also often form the basis of presentations to pupils in assemblies, and to both pupils and parents from outside speakers (in particular Karl Hopwood of E-Safety Ltd : http://esafetyltd.info/).

It is the responsibility of **all staff** to:

- report any concerns about appropriate filtering levels to the Director of Technical Support
- in line with the Prevent/radicalisation strategy, ensure that children are safe from terrorist and extremist material when accessing the internet in school
- be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce it through the curriculum
- report accidental access to inappropriate materials to the e-Safety officer in order that inappropriate sites are added to the restricted list
- report any incidents of cyberbullying, bullying or other inappropriate behaviour via the internet or other technologies to the College Deputy Head Pastoral or SMH Deputy Head

It is the responsibility of **pupils** to respect the requirements of the AUP; to report to staff any concerns or incidents they may become aware of which may compromise their online safety, or that of other users, and to ensure that their behaviour online adheres to the same high standards as are expected in their offline behaviour, both in school and at home.

Cyberbullying

The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyberbullying is a different form of bullying, which can happen 24/7, with a potentially bigger audience and more people involved as people forward content at a click.

Cyberbullying is the sending or posting of harmful or cruel texts or images using the internet or other (digital) communication devices.

There are many different types of cyberbullying:

- text messages - unwelcome texts that are threatening or cause discomfort.
- pictures/video-clips via mobile phone cameras - images sent to others to make the victim feel threatened or embarrassed.
- mobile phone calls - silent calls or abusive messages; or stealing the victim's phone and using it to harass others, to make them believe the victim is responsible.
- emails - threatening or bullying emails, often sent using a made-up name or someone else's name.
- chatroom bullying - menacing or upsetting replies to children or young people when they are in a web-based chatroom.

- instant messaging - unpleasant messages sent whilst children are having real time conversations online.
- bullying via websites - use of blogs (web logs), personal websites and online personal polling sites to spread upsetting lies about someone. This includes social networking websites such as FaceBook, Twitter, Tumblr, Instagram etc.

It is important to note that many aspects of cyberbullying outlined above are illegal under UK law, and the school has the right to read e-mail and other electronic communications and take action as a result of information obtained in this way.

In all incidents of cyberbullying, action will be taken in accordance with the Stonyhurst Anti-bullying Policy.