STONYHURST

AMDG

Academic Year 2021-22

CROSS CAMPUS E-SAFETY POLICY

Last Revised	May 2021
Revised By	▪ SMH Deputy Headmaster ▪ Director of Technical Services
Executive Lead	Bursar and Clerk to the Governors
Approval Body	Digital Strategy Steering Group
Date Approved	May 2021
Next Revision Due	May-June 2022
Persons Responsible for Next Revision	▪ SMH Deputy Headmaster ▪ Director of Technical Services
Policy Location(s)	▪ ISI Portal ▪ Stonyhurst Website ▪ Teams Channel

If you would like to request a printed copy of a policy, please contact the Compliance Manager j.mchugh@stonyhurst.ac.uk, the Headmaster's P.A. r.taylor@stonyhurst.ac.uk or the SMH Headmaster's P.A. t.ashton@stonyhurst.ac.uk

Contents

1. **INTRODUCTION** 3

2. **ROLES AND RESPONSIBILITIES** 3

Governors 3

Headmasters and DSLs 3

Director of Technical Support 3

PSHE Co-ordinators, Playroom Staff and Computing teachers 4

Staff 4

Pupils 4

3. **FILTERING** 5

4. **REPORTING** 5

5. **PARENT AWARENESS AND TRAINING** 6

6. **CYBER-BULLYING** 6

1. Introduction

1.1. 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.

1.2. 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 College, including in boarding areas.

1.3. 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)
- To undertake staff safeguarding professional development that includes online safety

2. Roles and Responsibilities

Governors

2.1. Have a responsibility to:

- Gain/develop an awareness of E-Safety as one element of the wider remit of safeguarding across the campus.

Headmasters and DSLs

2.2. Have a responsibility 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.

Director of Technical Support

2.3. Has a responsibility 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 constructive use of personal devices both in and out of the classroom
- ensure that all users are familiar with, and agree to, the Stonyhurst Acceptable Use Policy

PSHE Co-ordinators, Playroom Staff and Computing teachers

2.4. Have a responsibility to:

- ensure that up-to-date, age-appropriate E-Safety education is provided within the curriculum to pupils as they progress through the two Colleges. Details of the content and delivery 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 and SMH PSHE Programmes and appendices; and College and SMH Schemes of Work for Computing. 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.

Staff

2.5. Have a responsibility 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 College
- 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 Playroom Leader 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 (a) at the College to the appropriate member of the College HOP team or (b) at SMH to the SMH Assistant Head (Pastoral)
- undertake staff safeguarding professional development that includes online safety

Pupils

2.6. Have a responsibility to:

- respect the requirements of the Cross Campus Acceptable User Policy;
- report to staff any concerns or incidents they may become aware of which may compromise their online safety, or that of other users; and
- ensure that their behaviour online adheres to the same high standards as are expected in their offline behaviour, both in College and at home.

3. Filtering

3.1. The Colleges filtering systems blocks all sites on the Internet Watch Foundation (IWF) list, which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.

3.2. The College works with their respective providers to ensure that our filtering policy is continually reviewed and is in line with UK Safer Internet Centre and KCSIE 2019.

3.3. Stonyhurst's Synchronous Leased Line provision delivers speed to the maximum that our existing line allows and this includes a fully customisable layer 7 stateful Sophos XG firewall allowing for the highest level of threat detection and filtering, pre-configured to the latest DfE guidelines on protecting and monitoring internet usage.

3.4. The College has a clear procedure for reporting filtering breaches:

- If pupils discover unsuitable sites, they will be required to turn off monitor/screen and report the concern immediate to a member of staff.
- The member of staff will report the concern (including the URL of the site if possible) to a member of the Designated Safeguarding Team.
- The breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material that the College believes is illegal will be reported immediately to the appropriate agencies, such as: IWF, Lancashire Police or CEOP.

4. Reporting

4.1. Stonyhurst commits to take all reasonable precautions to ensure online safety but recognises that incidents will occur both inside College and outside College (and that those from outside College will continue to impact on pupils when they come into College. All members of the College are encouraged to report issues swiftly to allow these to be dealt with them quickly and sensitively through the College's escalation processes.

4.2. Any suspected online risk or infringement should be reported to the designated safeguarding lead on the same day – where clearly urgent, it will be made by the end of the lesson. Any concern/allegation about College staff misuse is always referred directly to the Headmaster, unless the concern is about the Headmaster in which case the compliant is referred to the Chair of Governors. Staff may also use the NSPCC Whistleblowing Helpline.

5. Parent awareness and training

5.1. The college runs a rolling programme of advice, guidance and training for parents to ensure that principles of e-safety behaviour are made clear, including:

- Information leaflets; in College newsletters; on the College web site;
- demonstrations, workshops, practical sessions held at College;
- suggestions for safe Internet use at home;
- provision of information about national support sites for parents.

6. Cyber-Bullying

6.1. The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside College. 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 with a click. During the current COVID-19 pandemic this is more prevalent.

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

6.3. 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.
- social media posts on platforms such as Instagram, Facebook, Snapchat, Twitter, TikTok etc.
- instant messaging - unpleasant messages sent whilst children are having real time conversations online.
- bullying via websites - use of blogs, vlog, personal websites and online personal polling sites to spread upsetting lies about someone. This includes social networking websites such as Facebook, Twitter, Tumblr, Instagram, Snapchat, WeChat, TikTok etc.

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

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

LDS