AMDG

STONYHURST

ICT Acceptable Use Policy / Online-Safety Policy

Stonyhurst College operates a campus wide ICT network. The Director of Technical Services has overall responsibility for these systems.

Name of Policy:	ICT acceptable Use Policy
Date of Policy Revision:	March 2018
Revised by:	Director of Technical Services IT Steering Group
Approved by:	Stonyhurst Governing Body
Date approved:	March 2018
Date of next revision:	April 2020
Location(s) where Policy can be found:	☐ ISI Portal ☐ College Website Y Intranet Y Hard copy files in the following offices: ❖ Compliance & Legal Support ❖ Headmaster's PA ❖ SMH Headmaster's PA ❖ Bursar's PA

Scope

1. This policy relates to the use of technology, including any devices which may be used for network, internet or email access (including Personal Computers, Laptops, Tablet devices, phones or games consoles), or the use of any internet or Stonyhurst College System

2. This policy applies to all students, staff, governors and visitors.

3. For the purpose of this policy it will be assumed that Stonyhurst refers to both Stonyhurst College and St Mary's Hall.

4. It applies to the use of technology on Stonyhurst College premises and also any use, whether on or off the premises, which affects the welfare of others or where the culture or reputation of the organisation are put at risk. The aims of this policy are:

a) to encourage students to make good use of the educational opportunities presented by access to technology;

b) to safeguarding and promote the welfare of students, in particular by anticipating and preventing the risks arising from:
   I. exposure to inappropriate material (such as pornographic, racist, extremist or offensive materials);
   II. the sharing of personal data, including images;
   III. inappropriate online contact; and
   IV. cyberbullying and other forms of abuse;

c) to minimise the risk of harm to the assets and reputation of the School;

d) to help students take responsibility for their own safety when using technology (i.e. limiting the risks that children and young people are exposed to when using technology); and

e) to ensure that students use technology safely and securely and are aware of both external and peer to peer risks when using technology.

5. This policy can be made available in large print or other accessible format if required.

Internet Access

6. The network also provides internet access, which is primarily provided for study by students at Stonyhurst College or St Mary's Hall. Reasonable personal use is permitted outside of normal study time provided it does not breach any other provisions of this policy. Controls and filtering systems are in place to prevent access to unsuitable material and control when students may access the internet. Access controls are also used to prevent access to internet services which could have a detrimental impact on the operation of our internet connection or internal network.

7. No attempts should be made to bypass or disable any security or control measures.

8. Students must not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. Use of technology in this way is a serious breach of discipline. Students must tell a member of staff immediately if they have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.

9. All users are expected to comply with Stonyhurst's E-safety policy.

10. All internet access, and attempted access, is logged for monitoring and safeguarding purposes. Reports are available to pastoral staff to allow scrutiny of individual internet use and will form part of the School's ongoing monitoring and review of safeguarding.

11. Privileged information regarding any aspect of organisation, or anyone associated with the organisation, should not be published anywhere on the internet unless specifically authorised to do so.

12. Derogatory or inflammatory comments regarding the organisation, or persons associated with the organisation, should not be posted on any internet site, including Facebook, Twitter etc. This applies to the use of Stonyhurst or personal computer equipment.

13. Attempted access to blocked websites is logged. Any user who believes that access to a particular site should be allowed may request that the website is unblocked. Such requests will be considered by the Director of Technical Services in consultation with other senior management, and if considered appropriate, access will be granted.

14. The provision of privileged internet access to individuals is not possible due to the detrimental impact such provision would have on system performance and support.

Guidance on social networking sites, applications and online groups may be found in Appendix 2.

Email

15. All students are provided with a Stonyhurst email account. Email is provided for work related activity, and to allow students to communicate with family and friends. Email may be monitored to investigate or detect unauthorised use and ensure the effective operation of the system.

16. Students must use their Stonyhurst email accounts for any email communication with staff. Communication either from a student's personal email account or to a member of staff's personal email account is not permitted.

17. Email carries the same legal status as other written documents and should be used with similar caution. Users have a responsibility to draft all emails carefully taking into account discrimination, harassment, defamation, and the need to maintain the reputation of The Trust. Material which would or place the reputation of Stonyhurst at risk should not be sent.

Appendix 1 outlines some good practice guidelines for email use.

18. Material that is libellous, indiscreet, offensive, or could jeopardise the welfare of others should not be sent. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist related nature, sexist, homophobic, any form of bullying, pornographic, defamatory or criminal activity. If students are unsure about the content of a message, they must speak to a member of staff.

19. Email which may contain sensitive information should not be forwarded without the permission of the sender.

20. Personal and confidential information should always be protected, even if it is received or discovered inadvertently. Receiving or using this kind of information may be unlawful under data protection legislation and laws relating to confidentiality.

21. The emails of others should not be read without their consent. This may constitute an offence under the Computer Misuse Act 1990.

22. Email attachments should not be opened if the identity of the sender is not known. Malicious attachments could place computers, email accounts, the Stonyhurst network or the reputation of Stonyhurst at risk.

23. During lesson or studies time students must only use email for study purposes or communication with teachers with the permission of the teacher or supervising member of staff.

Stonyhurst Network - security

24. Users must not share their passwords with anyone else, be it internal or external, nor should a user log on with another user's credentials. This includes assuming another user's online identity or attempting to gain a higher level of access to campus systems.

25. Users should be encouraged to change their passwords regularly. Passwords should be complex, should be at least 6 characters in length and contain numbers, letters and special characters. Passwords should not be changed by simply changing a preceding character. Should you suspect that your password is known to others, please contact the Technical Support Team.

26. Users should ensure that any workstation left unattended is left in a secure state, either logged off or locked.

27. Any activity undertaken by users should in no way knowingly compromise the security of the campus network. This includes installing any software without the consent of the Technical Support department, and knowingly infecting the network with a botnet, virus, trojan, adware or malware.

28. Users connecting their own devices to the campus network should ensure that they have

adequate protection installed on these devices, including anti-virus protection and all relevant system and security updates from the relevant hardware and software vendors. Systems not meeting these criteria will have restricted access to campus systems. Should you have any concerns regarding device security please contact the Technical Support Team.

29. The privacy of other users should be respected and no attempts to access, modify or copy data or passwords belonging to others should be made.

30. Unauthorised hardware should not be connected to any part of the Stonyhurst Network or telephone system.

31. Exploitation of information available on Stonyhurst systems, especially for commercial purposes, is forbidden.

Monitoring and Privacy

32. Title to all data produced, accessed, stored and viewed on campus systems belongs to Stonyhurst. As such Stonyhurst reserves the right to access and view all data either accessed or stored, including email.

33. All campus workstations have active monitoring software installed, with the capability to remotely monitor activities in real time.

34. All Campus internet access is filtered in line with agreed national educational standards. This is also monitored and logged. Given the nature of the internet, whilst every reasonable effort is made to avoid inappropriate material being accessed, the College cannot guarantee this.

35. Access to any of the above information or monitoring activities will only be at the request of the Director of Technical Support and/or a member of the Senior Management Team. All activities will be recorded and should it be deemed necessary, information will be passed on to appropriate authorities for further investigation.

36. Should inappropriate behaviour be discovered or suspected, the College reserves the right to fully investigate. This may include the seizure of equipment, both college and privately owned, held on the premises.

Inappropriate Behaviour

37. Do not engage in activities which would bring the name of Stonyhurst College or any person or entity connected to Stonyhurst College into disrepute.

38. Do not use indecent, obscene or offensive language in any form of communication.

39. Users should not use any device or software to cause offence or upset to any person or entity.

40. Campus systems should not be used for accessing inappropriate materials such as, but not limited to, pornography, dating and gambling.

41. Do not use 'proxy bypass' software or websites to circumvent campus internet filtering systems.

42. Do not use 'peer-to-peer' software such as BitTorrent on any device present on the Campus.

43. Do not download or use any media or software that breaks UK and International Copyright and Licensing laws.

44. Do not take or share the media of other staff or pupils without their knowledge or express permission.

45. Do not share any information of a personal nature about yourself or another person with anybody, excepting normal campus operations including UCAS and the Health Centre.

46. Should you inadvertently contravene any of the above, please contact the Technical Support Team ASAP.

Best Practices

47. All users should be aware that their activities in the online world will be judged in the real world.

48. College equipment can only be used for recreational purposes outside of lesson and study time.

49. All users should use the printing facilities economically for educational purposes or other purposes as agreed with your teacher or line manager. Large print volumes should be directed to the Campus MFP printing service.

50. Campus email should be checked on a daily basis as this is a main route of communication on Campus. Should assistance be required for setting up email on your own devices please see the Technical Support Team.

51. All computer rooms should be kept tidy. Food and drink are not permitted. Please leave the room as you would wish to find it.

Mobile electronic devices

52. Stonyhurst College and St Mary's Hall recognises the importance of emerging technologies available in modern mobile devices e.g. camera, video and sound recording and internet access. Students may have the opportunity to use their mobile devices in the lessons. On these occasions students may do so only when express permission has been given by the teacher.

53. Mobile devices should be switched off and kept out of sight during lessons, supervised study sessions, studies and in the library unless permission has been given. If permission is given by a member of staff, the mobile device must not disrupt student learning.

54. Unless permission has been given, mobile devices should be switched off and kept out of sight as outlined in paragraph 31 and should not be used to make calls, send SMS messages, surf the internet, take photos, listen to music or access other applications during lessons, study, studies or in the library. Should there be disruptions caused by a mobile device, it will be confiscated and handed into the Deputy Head Pastoral's Department where it will be stored securely and then returned after an appropriate period of sanction.

55. Using mobile devices to bully and threaten other students is unacceptable and will not be tolerated. In some cases it can constitute criminal behaviour. The mobile device will be confiscated and the School Reward and Sanctions Policy adhered to. Devices may be searched in appropriate circumstances.

56. Use of electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not the student is in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use (see the School's Anti-bullying Policy and Behaviour Policy) and the School's safeguarding procedures will be followed in appropriate circumstances (see the School's Child Protection Policy).

57. Students may only use cameras or any mobile device with the capability for recording and / or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image.

58. It is forbidden for students to target another student and use their mobile devices to take videos and pictures of acts to denigrate and humiliate that student and then send the pictures to other students or upload it to a website for public viewing. This also includes using mobile devices to photograph or film any student or member of staff without their consent. It is a criminal offence to use a mobile device to menace, harass or offend another person.

59. Mobile devices are not to be used or taken into changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to fellow students, staff or visitors to the school.

60. Students are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the School and may constitute a criminal offence. The School will treat incidences of sexting (both sending and receiving) as a safeguarding matter under the School's child protection procedures (see the School's

Child Protection Policy). Students concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

Cyber-Bullying

Cyber bullying is bullying which occurs by the use of electronic media such as mobile phones, cameras, email, and the internet. This could include any of the following:

- Bullying by texts, messages or calls on mobile phones
- Use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites
- Hi-jacking email or other online accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat-rooms or other online facilities

61. Individuals will be held personally responsible for all material they have placed on a website and for all material that appears on a website where they are the account holder. Misconduct of this kind while away from Stonyhurst may give rise to disciplinary action if the welfare of others or the culture or reputation of the organisation is placed at risk.
62. Stonyhurst routinely monitors use of the internet and email for abuse, and reserves the right to examine mobile phones, laptops or other devices where there is reason to suspect abuse.

Appendix 3 provides some further guidance on cyber-bullying.

Ownership of Systems and Programmes

63. All computer programmes or systems developed or generated as a result of employment by Stonyhurst College or by the use of the Stonyhurst's hardware or software, will be the property of Stonyhurst College.

Procedures

64. Any breach of this policy may incur disciplinary action. Any misuse of technology by students will be dealt with under the School's Rewards and Sanctions Policy.

65. Students must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-bullying Policy. If a student thinks that he / she might have been bullied or that another person is being bullied, he / she should talk to a teacher about it as soon as possible. Appendix 3 of this policy provides further guidance about cyberbullying.

66. Where there is concern that a student is suffering, or is likely to suffer significant harm, this will be addressed as a child protection incident under the school's Child Protection Policy.

67. In a case where the student is considered to be vulnerable to radicalisation, they will be referred to the Channel programme. Channel is a programme which focuses on support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

Sanctions

68. Where a student breaches any of the School rules, practices or procedures set out in this policy, the Governors have authorised the Headmaster to apply any sanction which is appropriate and proportionate to the breach in accordance with the School's Rewards and Sanctions Policy including, in the most serious cases, expulsion. Any action taken will depend on the seriousness of the offence.

69. Unacceptable use of electronic devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material.

70. The School reserves the right to charge a student or his / her parents for any costs incurred to the School as a result of a breach of this policy

Monitoring and review

71. All serious incidents involving the use of technology will be logged in the Discipline Log

72. The Deputy Head (Pastoral) has the responsibility for the implementation and review of this policy and will consider the Discipline Log and the logs of internet activity (including sites visited) as part of the ongoing monitoring of safeguarding procedures, to consider whether existing security and e-safety practices within the School are adequate.

73. Consideration of the efficiency of the School's e-safety procedures and the education of students about keeping safe online will be included in the Governors annual review of safeguarding.

Staff Use of Social Media

74. The following guidance is provided with the intention of protecting the best interests of members of staff and the School.

75. There are two main kinds of online activity with which this guidance is concerned:
- These are private personal activity, involving friends and contacts
- Activity carried out on behalf of Stonyhurst

As a matter of best practice members of staff should keep personal and school-related activity separate.

Private personal activity, involving friends and contacts

76. Staff are not discouraged from using social media and engaging in other online activity. However, as a Stonyhurst member of staff, and especially as someone working in education, great care should be taken when posting anything on the internet

77. Staff are reminded that, even though you are acting in your own private personal capacity, you are 'on show' as a representative of Stonyhurst to colleagues, parents, pupils and any anyone else who goes online. Staff are members of the Stonyhurst / St Mary's Hall community, even though their digital account(s) is/are not linked to the School.

78. Private personal activity should not be carried out under or in the name of Stonyhurst.

79. Staff should not say anything that compromises their role at Stonyhurst. Specifically staff should not:

- Bring the School into disrepute
- Criticise your colleagues or the School
- Post photographs of, or information about staff, pupils or parents
- Reveal confidential school information
- Communicate with pupils via any private personal account, other than your Stonyhurst / St Mary's Hall account.
- Join any online "group" where workplace issues specific to Stonyhurst / St Mary's Hall may be discussed, except where that group is hosted on a school system.

Activity carried out on behalf of the School

80. The School recognises the value of social media and other online activity, both as an educational resource and as a way of promoting the School.

Key principles which apply to social media activity carried out on behalf of the School:

- The relevant Head of Department/ Pastoral Head is responsible for the content
- The role of running a departmental account must not be delegated to a pupil
- Spelling and grammar remain important when representing Stonyhurst.
- All social media activity should reflect and focus on areas relevant to the role or specialism of the department, avoiding personal interests or unrelated issues
- Content should take account of the intended audience
- All accounts used for school-related activity are owned by Stonyhurst.
- All accounts must be registered with the Director of Marketing who should also be provided with details of usernames and passwords.

Using Twitter or Facebook on behalf of the School

81. Any member of staff who would like to set up a Departmental account on behalf of the School should consult the Director of Marketing.

82. Departments are welcome to use Twitter / Facebook, provided that they act in accordance with the guidance given above and, in addition, the following:

- Correct spelling and grammar is essential, even in 140 characters
- The regularity of Tweets / Facebook posts should be carefully considered.
- Departmental Twitter feeds must be regularly updated, with a minimum of four/five Tweets per week.
- Facebook posts should take place at least once a week.
- If there is not enough regular content, the account may be closed down by the Director of Marketing
- Anyone wishing to set up a Departmental account should consider if they will have enough content to meet the minimum requirements or whether it would be better to supply material for the main @Stonyhurst account.

83. The username and password of each departmental Twitter account must be shared, securely with the Director of Marketing

84. In the interests of safeguarding, no member of staff or Departmental account should ever follow the Twitter or Facebook account of any Stonyhurst pupil, or send them a Direct Message.

85. For consistency, accounts must use the naming convention @Stonyhurst_name of department (for example @Stonyhurst_Art), and the homepage should state 'Tweets by Stonyhurst insert name Department' (for example 'Tweets by the Stonyhurst Art Department'). A Stonyhurst email address and contact number may also be included.

86. For Facebook pages specific title pages should read exactly as "Example, Stonyhurst College". An example would be "Grammar Playroom, Stonyhurst College" Please note the position of the comma; without any full stops. For continuity it is important that all staff for this format exactly.

87. In addition to page titles URL's must be set to a standard format across all Stonyhurst / St Mary's Hall pages. URL's should be in the example format of "grammarplayroom.stonyhurst

88. All Facebook pages should have a short description included. All descriptions must be referred to the Director of Marketing to review for continuity.

89. All parents / guardians will be given the opportunity to refuse permission for their son/daughter to be shown on Facebook / Twitter. This will be done via a check box question on the admissions enrollment forms.

Appendix 1

Email Guidelines

1. A meaningful subject should always be included: e.g. History Studies for Tuesday is more useful than Studies.

2. Politeness is desirable at all times. Care should be taken to ensure that accepted courtesies (such as an opening greeting and a closing remark) are observed as a matter of course. For students, greetings such as Dear Sir, Dear Mrs Smith or Dear Fr Twist are appropriate for staff whereas Hi may be appropriate for friends or family.

3. Sensitivity should be shown and appropriate language used. The meaning and context of the email may be misunderstood as the recipient cannot see the sender nor hear their tone of voice.

4. Emails should always be proof read before sending: errors in spelling, poor grammar or words missing suggest lack of interest or respect for the recipient.

5. Email distribution should be restricted to those who need to read it and the inappropriate use of Reply to All should be avoided.

6. The privacy of an email cannot be guaranteed; some recipients may inappropriately forward to others.

7. Unnecessary emails should be regularly deleted.

8. Multiple messages should not be sent to one person as a means of asserting a point of view. This may be seen as harassment or bullying.

Appendix 2

Social Networking Sites

1. Social networking sites such as Facebook provide dynamic new ways of communicating with friends and family around the world. However these sites can unintentionally expose far more personal details to the outside world than is desired. This could compromise reputation, bring Stonyhurst into disrepute or provide opportunities for identity theft.

2. The rapidly changing nature of these sites makes it difficult to give specific guidelines and the following are intended to help avoid problems. Facebook is used as the example; however the same principles should be applied to any other site that is used.

3. Students may make reasonable use Facebook outside of work or study times.

4. Online profiles should only show information which the owner is comfortable sharing with others, including personal details and postings.

5. Personal details regarding sexuality, politics or religion should not be publicised as this may cause regret at a later date.

6. Derogatory or offensive remarks regarding any person or organisation should not be posted.

7. Embarrassing or compromising photographs of yourself or others should not be posted.

8. Messages which could incite or suggest unacceptable or criminal behaviour should not be posted.

9. Students are advised to add themselves to the Stonyhurst College network which allows them to be found more easily by friends.

10. Profile privacy settings should be set so that personal details and postings are only visible to friends.

11. Profiles should be set so that the user can only be found by friends and selected network members.

12. Friends should be known to the user.

13. Students must not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons.

Applications

14. Caution should be exercised when considering the use of an online Application. Signing up for an Application often means that the Application owner has permission to use personal details and send messages or postings in their name. There are a number of malicious Applications available on Facebook; if in doubt do not sign-up to an Application. An Application cannot be presumed to be safe simply because a trusted friend has sent it to you; friends may be the victim of a malicious Application.

Groups

15. When considering joining a Group check which type it is. If it's a global group and open to anyone to join then look carefully at the postings before a decision is made to join. Individuals have no control over who reads postings to this group. If the Group is closed there will be some measure of control by the Administrators and applications will have to be made to join the group.

16. If the title of a group is offensive to an individual, group or organisation then it should not be joined. A group may be a pretending to be an official group, intended to deceive people into believing it is genuine. These groups are often used to slander or discredit others and risk prosecution if postings are libellous. When considering joining any Group it is important to look at the type of postings on the group, before deciding to become associated with it. Any concerns about the type of postings within a group should prompt the immediate leaving of the group.

17. Any individual setting up a Group will be responsible for everything that is posted on that Group. It is recommended that any Group created is closed to allow all members to be approved.

18. Group Title and Description are visible to everyone with a Facebook account. If the title or description is defamatory towards an individual or group then it could be cause for legal action against the administrator and members.

I, …… (PRINT NAME)

have read, understood and agree to abide by the Campus Acceptable Use Policy set out above.

Signed …… Stonyhurst No. ……

Date ……

Appendix 3

Guidelines of Cyber-Bullying

Avoid being a Cyber-Bully

1. Before sending a message to anyone, or posting a comment on a website about anyone, it is important to ask if the sender would be happy to receive such a message, or see such a comment about him/her. If not then the message or post should not be sent.

2. Think before you send - whatever you send can be made public very quickly and could stay online forever.

Dealing with Cyber-Bullying

3. All the normal rules for dealing with bullying apply in accordance with the Anti-bullying Policy. If you are being bullied, or you know of someone else being bullied report it to a teacher or Playroom Master / Housemistress or any other adult you trust.

4. It is important not to reply or retaliate to bullying or abusive messages or images, or forward them to anyone. However they should be kept as evidence.

5. Block the bully. Most social media websites and online or mobile services allow you to block someone who is behaving badly.

6. Passwords or passcodes to your mobile, email or other online accounts should never be given to others.

Useful resources

http://www.safetynetkids.org.uk/

http://www.thinkuknow.co.uk

www.childrenscommissioner.gov.uk