ICT Usage Policy

1) St. Michael's College is committed to the ethical and moral use of all Information Technology.

2) To security of information, St. Michael's College is continually developing and managing the information security environment to comply with the highest standards.

3) St. Michael's College is supportive of, and committed to maintaining high standards of information security and views information security as essential to the long- term goals and strategic objectives within the College.

4) St. Michael's College wishes to ensure and demonstrate compliance with all relevant legislative, regulatory and contractual requirements.

The purpose of the policy

5) The purpose of the policy is to define the way in which electronic communications are managed in the College and the rights and responsibilities of those managing areas and of all users.

Acceptable Usage Policy

This ICT Usage Policy applies to the students, employees and volunteers at St. Michael's College and all other persons offered access to College Information and Communication Technology (ICT) systems. (The term 'User' refers to all).

Scope

6) This policy applies to all users of St. Michael's College's Information and Communications Technology resources, both on and off site, within and outside of normal working hours.

7) The policy covers the appropriate use of such technology and the College's right to log and monitor any such activity including details such as the content of emails, which sites are visited and what is downloaded. Each user is responsible for being fully aware of the ICT Usage Policy and its implications for personal conduct.

8) As in all their work activities, users are required to use ICT resources in a reasonable, professional, ethical and lawful way.

General Principles of Acceptable Usage Policy

9) St. Michael's College's ICT systems, resources and associated applications are intended for activities that support the mission, goals and objectives of the College. This usage is encouraged and supported.

10) The ICT systems, resources and associated applications are to be used in a manner consistent with the College's mission and values and as part of the normal duties of all persons offered access to the College's (ICT) systems.

11) The College's email accounts, Internet identifications and web pages should only be used for appropriate and sanctioned communications.

12) The use of the College's, resources and associated applications may be subject to monitoring for security and/or network management reasons and as a result users may also have their access and use restricted. At St. Michael's College use of internet software is used to monitor access to websites.

13) The distribution of any information through the Internet, email and any messaging systems through the College's network are subject to scrutiny by appropriate personnel.

14) It is the responsibility of each member of staff and user to protect the information or information assets under their direct control and to adhere to the established information security policies and procedures when conducting their duties. Breach of information security policy and procedures may result in disciplinary action up to and including dismissal/expulsion.

15) Users have a personal responsibility to report any information security incidents or suspected weaknesses to the Principal/Deputy Principal or any member of the ICT team at the first opportunity.

16) Users are asked to report and look for assistance if they access material or receive a message that is inappropriate. They should contact any member of the ICT team.

17) Users must not access, download or send any material through ICT technology which:
    - Is offensive or could give rise to offence being taken by a 'reasonable person',
    - Is illegal
    - Could bring the College into disrepute

18) The use of all ICT systems, resources and associated applications are subject to Irish and European law and any illegal use will be dealt with appropriately through the College's disciplinary process.

19) St. Michael's College is committed to ensuring that it operates in compliance with the Data Protection Acts 1988 and 2003. St. Michael's College makes every effort to ensure that personnel information is maintained in a manner which is accurate, relevant and is held securely at all times. All those maintaining records on behalf of the College are asked to ensure that they adhere to the provisions of the Data Protection Acts.

20) The College retains the right to report any actual or potential illegal violations to the relevant State and other Authorities.

Individual Practice

21) **Access and Passwords:** Those in charge of any area need to ensure that all computer access is password protected. Good practice would suggest the following guidelines:

    - Each individual should have their own password.

- Passwords should never be shared (but disclosed to the ICT Coordinator when necessary) and should be changed at regular intervals and not be reused. Managers of computer systems are required to hold a record of all access passwords in an area at all times, in a secure location

- Users undertake not to go beyond or attempt to go beyond their authorised access.

22) **Internet Access**: Each person using the internet does so under their password and hence will have responsibility for illicit use of that password with or without their consent. Internet Access is conditional on the following additional rules being observed:

    Where internet access is available to particular employees / persons the internet is for the College's business only. Users who in the opinion of management, have abused this, will be subject to disciplinary sanction.

    To access, download or send any indecent, obscene, pornographic, sexist, racist, defamatory or other inappropriate materials, as well as the circulation of such materials, will be a serious offence, which may result in expulsion or dismissal. This rule will be strictly enforced and is viewed as very serious with potential criminal liabilities arising there from. The Gardaí or other appropriate authority will be informed, where appropriate.

23) Software and Hardware: Users should not attempt to disrupt the computer system by interfering with software or hardware. No deliberate attempt must be made to introduce software of any kind, including games on to the system without the expressed permission of the ICT Coordinator

24) **Password-protected screensaver**: Users should ensure that their computer is protected by a password-protected screensaver when it is left unattended.

25) **Data Storage:** Where available, staff should save their work files on the local server to ensure that it is backed up by the server. In the instance of a local server not being available, staff must ensure that critical data is backed up by consulting with their manager and making appropriate arrangements for data backup.

26) **Moving Data Off-site / USB Keys:** Users must show due diligence when transferring, carrying and using any electronic data off the St. Michael's College systems e.g. working on home PCs. St. Michael's College has a legal obligation to protect its data content and has no ability to control data on personal PCs. Therefore, it cannot be emphasised strongly enough, that the use of USB / Memory sticks to transfer confidential information must be treated with great caution. The use of encrypted USB keys is highly recommended.

27) **Personal gain or profit:** Users may not use the ICT system for unauthorised and unapproved commercial purposes or personal gain or profit.

28) **Users should not subscribe** to electronic services or other contracts on behalf of St. Michael's College unless with the express authority to do so.

29) **Users will respect the rights of copyright owners**. Copyright infringements occur when one inappropriately reproduces a work that is protected by a copyright.

30) **The use of photographic images** or film on behalf of the College should respect copyright obligations and be appropriate for use, consistent with the ethos of the College.

31) **Risk of Harassment** Users will not use the ICT systems to access, download or send any material that could be found to be inappropriate or offensive by others, i.e., material that is obscene, defamatory or which is intended to annoy, harass or intimidate another person or advocates discrimination towards other people. This could be regarded as harassment or bullying and would be dealt with according to the Dignity at Work policy and disciplinary code.

32) **Users will not use the ICT systems to access, download or circulate material** that contains illegal or inappropriate material such as obscene, profane, objectionable or pornographic material or that advocates illegal acts or that advocates violence.

33) **ICT facilities should not be used** to make or post indecent remarks, proposals or any material which may bring the College into disrepute.

34) **It is not permissible to advertise** or to otherwise support unauthorised or illegal activities.

35) **Inappropriate Language:** Users will not type, record or reproduce obscene, profane, lewd, vulgar, rude, inflammatory, racist, threatening or disrespectful language or images on the computer system. Information which could cause damage, danger or disruption will not be posted. Users will not knowingly or recklessly post false or defamatory information about a person, group or organisation. Users will not engage in defamatory or personal attack, prejudicial or discriminatory, that distress or annoy another person.

36) **Should students cause damage to the ICT system, they are required to bear the cost of repairs/replacement.**

The use of Email and other computer based Communications:

There are risks attached to the sending of E-mails such as:

37) A message may go to persons other than the intended recipient and if confidential or sensitive this could be damaging to the College.

38) E-mail messages can carry computer viruses dangerous to computer operations generally.

39) Letters, files and other documents attached to E-mails may belong to others and there may be copyright implications in sending or receiving them without permission.

40) E-mail messages written in haste or written carelessly are sent simultaneously and without the opportunity to check or rephrase. This could give rise to legal liability on the College's part such as claims for defamation, etc.

41) An E-mail message may legally bind the College in certain instances without the proper authority being obtained internally.

42) It should be remembered that all personal data contained in E-mails may be accessible under Data Protection legislation and, furthermore, a substantial portion of E-mails to Government and other public bodies may be accessible under Freedom of Information legislation.

43) E-mails should be regarded as potentially public information which carry a heightened risk of legal liability for the sender, the recipient and the organisations for which they work.

To reduce the risks inherent in the use of E-mail the following guidelines are necessary:

44) **Users should only use approved e-mail accounts (i.e. @stmichaelscollege.com) on the school system for purposes related to their work at St. Michael's College.**

45) The use of BCC (Blind Carbon Copy) for internal communication is not permissible to prevent flame attacks.

46) Particular care should be taken when sending confidential or commercially sensitive information. E-mail is neither a secure nor a private medium. If in doubt please consult a member of the IT team.

47) Care should also be taken when attaching documents as they may give rise to the release of information not intended, therefore it is important to vet attachments. The ease with which files can be downloaded from the Internet increases the risks of infringement of the rights of others particularly the intellectual property and other proprietary rights. If in doubt please consult your manager.

48) An E-mail should be regarded as a written formal letter, the recipients of which may be much wider than the sender intended. Hence, any defamatory or careless remarks can have very serious consequences as can any indirect innuendo. Inappropriate remarks whether in written form, in cartoon form or otherwise must be avoided, as should any remarks that could be deemed indecent, obscene, sexist, racist or otherwise offensive or in any way in breach of current legislation.

49) Should you receive any offensive, unpleasant, harassing or intimidating messages via the E-mail you are requested to inform the Principal/Deputy Principal or any member of the ICT team.

50) Any important or potentially contentious communication which you have received through E-mail should be printed and a hard copy kept. Where important to do so you should obtain confirmation that the recipient has received your E-mail.

51) Documents prepared for your service users may be attached via the E-mail. However, excerpts from reports other than our own, if substantial, may be in breach of copyright and the author's consent ought to be obtained particularly where taken out of its original context. Information received from one service user / client should not be released to another service user / client without prior consent of the original sender - if in doubt consult your manager.

52) **The Use of Other Technologies including Web2 applications such as Facebook and Twitter.**

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in the College is allowed.

- Staff must inform the ICT Coordinator if they wish to use a Web 2 or any new webbased ICT program.

- Staff should not give out their personal email addresses, skype addresses, facebook address or any such personal point of contact to students. If a web application has been approved the staff member should set up a new account solely for educational purposes, alert the ICT Committee of the account name and practice due diligence in how it is used at all times. If any inappropriate communication arises from such an application they should treat it as they would an inappropriate email and contact a member of management. It is vital that all such applications be used with the regulations for email in mind in terms of writing, responding

and remembering that they are reflecting on the St. Michael's College name and reputation. It is also important that students are not leaving a digital footprint which could leave them vulnerable.

- Please note that any external communication tools such as blogs etc are a special case and must be presented to the Principal.

Newsgroups and Chat Rooms

- Access to Newsgroups will not be permitted to staff unless an educational requirement for their use has been demonstrated. If users are part of a newsgroup they must inform the ICT Coordinator Too much email generated by Newsgroups can overload the mail server (when your mail storage capacity is reached you will no longer receive email).

- Staff should use only regulated educational chat environments while at school.

- Staff, directing students to chat rooms, will fully evaluate these chat rooms before allowing access to their students, including any hyperlinks attached to these sites. They will also advise students to use pseudonyms and to never use their photo in such correspondence.

In general when using ICT systems, users must not

53) Represent personal opinions as those of the College. All staff and other users are instructed to use a disclaimer such as:

> "The information in this e-mail is confidential and may be legally privileged. It is intended solely for the addressee. Access to this e-mail by anyone else is unauthorised. If you are not the intended recipient, you are notified that any disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited. Any views, opinions or advice contained in this e-mail are those of the sending individual and not necessarily those of the College. It is possible for data transmitted by e-mail to be deliberately or accidentally corrupted or intercepted. For this reason where the communication is by e-mail, St. Michael's College does not accept any responsibility for any breach of confidence which may arise from the use of this medium."

54) Represent yourself as someone else.

55) Forward chain emails.

56) Waste time by using the Internet and email systems for non-school related activities.

57) The College reserves the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail system for any purpose

58) Perform any other inappropriate uses identified by the College.

Confidentiality

59) Notwithstanding the College's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorised to retrieve or read any e-mail messages that are not sent to them. Any exception to this policy must receive prior approval from the ICT

Coordinator. However, the confidentiality of any message should not be assumed. Even when a message is erased it is still possible to retrieve and read that message. If any breach of our E-mail policy is observed then disciplinary action up to and including dismissal/expulsion may be taken.

60) Users must not upload, download or otherwise transmit commercial, unlicensed software or any other copyrighted materials that belongs to the College or external parties.

61) Users must not reveal, publicise or disclose any information that might be in breach of the Data Protection legislation

62) Users must not reveal or publicise confidential or proprietary information that includes, but is not necessarily limited to, all types of educational or financial information, strategies and plans, databases and the information contained therein or any other information which is deemed the property of the College.

63) Send confidential emails without applying appropriate security protocols.

Security

64) All PCs must have virus detection software installed; users must not attempt to investigate virus programmes themselves.

65) To prevent computer viruses from being transmitted care must be exercised by users in the downloading of material. It should be from a reliable source and the user must not seek to avoid the standard virus protection measures implemented by St. Michael's College. Staff must ensure that virus protection on personal devices is up-to-date to avoid brining viruses into the school.

66) It is essential that only software that is authorised, licensed and approved is installed on St. Michael's College equipment, and that licence agreements are complied with.

67) Users must not intentionally interfere with the normal operation of the College ICT systems, resources and associated applications. This includes the distribution of computer viruses and sustained high-volume network traffic that substantially hinders other users of the network.

68) It is not permitted to examine, change or use another person's username, password, files or outputs for which no explicit authorisation has been given.

69) Care must be taken that mobile devises are secure at all times and that no confidential data is stored on them. They should be locked away when not in use and user –ids or passwords should not be stored with the devise.

70) Care must be taken that all documents and computer media are disposed of securely at the end of their life, shredded or sent to secure disposal as appropriate.

71) All computers in the offices of the College should be monitored regularly to ensure that they are being used in accordance with the stated policy. Where there is any suspicion or doubt a person with specialist knowledge of computer hardware and software should be asked to assess the purposes for which the computer has been used.

Safeguarding Children

72) Students should be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Ensuring students are aware of the SMART rules and are aware of how to use the Internet effectively is the responsibility of all teachers.

73) Teachers must be aware of the regulations regarding the use of Web 2 applications and email and seek to protect students and themselves in this regard.

- Where a computer is used by more than one person, each person should be obliged to have a unique username and password, or where this is not possible, to maintain a signed record of the date, time and duration of their use of the computer.

- Where a computer can be accessed by children or young people, it should be accessible only through the use of a username and password unique to each child. Where this is not possible, the children or young people should be obliged to provide a signed record of the date, time and duration of their use of the computer and their access should be supervised at all times.

- Computers which can be accessed by children or young people should always employ appropriate filtering software.

- All the computers in the College are monitored regularly to ensure that they are being used in accordance with the stated policy. Where there is any suspicion or doubt, a person with specialist knowledge of computer hardware and software should be asked to assess the purposes for which the computer has been used.

- St. Michael's College should continuously evaluate the possible ways that students communicate with staff, volunteers and each other, such as via the internet, mobile phones, email using digital and other electronic or information technology.

- It is important to develop guidance to reduce the risks to children that may arise in the course of their use of technology. Such risks include:

    - being groomed online by paedophiles
    - experiencing or perpetrating bullying
    - accessing or being exposed to inappropriate or harmful material
    - having their personal contact details accessed and circulated
    - Having personal images uploaded and used without consent.
    - The College needs to consider how its personnel use images (such as photographs and film) of children in publications or on websites.

Protect Your Reputation and your Career

74) It is essential that all personnel and other users adhere to this ICT Usage Policy or risk disciplinary action in line with the College's codes of conduct.

75) Please see form of Acceptance below which should be signed by each user.

76) This policy will be reviewed and updated as required

FORM OF ACCEPTANCE

I have read ICT Usage Policy of St. Michael's College and confirm my acceptance and adherence to this document.

Signed: _____ Date: _____