INFORMATION AND COMMUNICATIONS TECHNOLOGY (I.T.)

[June 2012]

Acceptable Use (IT) Policy of

Coláiste Mhuire Co-Ed, Thurles

INFORMATION AND COMMUNICATIONS TECHNOLOGY (I.T.)

[June 2012]

Acceptable Use Policy of Coláiste Mhuire Co-Ed, Thurles

Table of Contents

The purpose of the policy

1. 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 all departments of the college (both administrative and academic) and of all users.

Acceptable Usage Policy

This Acceptable Usage Policy (AUP) applies to the students, employees and volunteers at Coláiste Mhuire Co-Ed and all other persons offered access to College Information and Communication Technology (I.T.) systems. (The term 'User' refers to all.). This document will appear on the school website and access to the full document is available for staff, students and parents using this medium. Upon request, hardcopies can be supplied. An abridged version of this policy is printed in the student diary. Students/parents are also requested to sign this annually through the student diary.

Scope

2. This policy applies to all users of Coláiste Mhuire Co-Ed's Information and Communications Technology (I.T.) resources, both on and off site, within and outside of normal working hours. It also applies to all communication regarding Coláiste Mhuire and its users within and outside of normal working hours.

3. The policy clarifies that the Information and Communications resources are in place to meet the communication, administration, pedagogical and learning and teaching needs of the College. These resources include hardware, software, user accounts, local and wide area network facilities as well as services accessed via the Internet. Coláiste Mhuire Co-Ed encourages its staff and students to use these resources in a manner which will facilitate their work and education.

4. 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 must take responsibility to make themselves aware of the College Acceptable Use Policy and its implications for personal conduct.

5. As in all their work and school activities, users are required to use I.T. resources in a reasonable, professional, ethical and lawful way. Computing resources must not be used for any illegal or unethical purpose and should not be used for recreational or personal use.

General Principles of Acceptable Usage Policy

6. Coláiste Mhuire Co-Ed's I.T. 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. Computing resources must not be used for any illegal or unethical purpose and should not be used for recreational or personal use.

7. The I.T. 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 (I.T.) systems.

8. The use of computing resources is subject to the regulations and guidelines outlined in this document.

9. It is the responsibility of the individual to be aware of the regulations and guidelines. Ignorance of the regulations and guideline sis not acceptable as an excuse or defence.

10. All College online communications including email accounts, Internet identifications and web pages should only be used for appropriate and sanctioned communications.

11. 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.

12. Staff and students are advised that using their own devices in school are governed by this policy. In addition the unauthorised connection of personally owned devices to the school network is strictly prohibited. All students' personal computers/network-capable devices must be registered with the ICT Coordinator at time of introduction and re-registered at the start of the academic year thereafter. Unregistered computers may be confiscated. Any access to the network from a smartphone or digital device must be used with the user name and password of the owner of the smartphone or tablet computer. Any access by another user on a smartphone or tablet computer not owned by them will be an offense, and both the owner and the user will be in breech of the College's IT policy.

13. The distribution of any information through the Internet/Intranet (this includes facebook, youtube, twitter and any other web2 technology), 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 when conducting their duties. Users

must not interfere or attempt to interfere in any way with data belonging to another user. No user should access or make unauthorised copies of data belonging to another user. 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 I.T. team at the first opportunity.

16. Users are asked to disconnect immediately, report and look for assistance if they access material or receive a message that is inappropriate. They should contact the Principal/Deputy Principal or any member of the I.T. team.

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

18. Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that waste computer resources or unfairly monopolise resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files (including music and video), accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

19. The use of all I.T. 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.

20. Coláiste Mhuire Co-Ed is committed to ensuring that it operates in compliance with the Data Protection Acts 1988 and 2003. Coláiste Mhuire Co-Ed makes every effort to ensure that personal 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. [For further information see the colleges Data Protection Policy on the school website]

21. The College retains the right to report any actual or potential illegal violations to the relevant State, International and other Authorities.

Individual Practice

22. Personal Safety: The User:
    - will not post personal contact information about himself or other people.

Personal contact information includes address, telephone, school address, work address, photograph etc.

- will not agree to meet with someone contacted online.
- will not sign a 'guest book' on a Web page on behalf of Coláiste Mhuire Co-Ed.
- will promptly disclose to the Principal or the Deputy Principal, any message received that is inappropriate or which makes you feel uncomfortable.
- will not use artefacts associated with the college (e.g. the College Crest) or personal web spaces/pages.

23. 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:
    a. Each individual should have their own password.
    b. Passwords should never be shared* (but disclosed to the ICT Coordinator when necessary) and should be changed at regular intervals and not be reused.
    c. Passwords should be at least 6 characters long. Ideally use a combination of capitals and lower case, letters and numbers.
    d. Users undertake not to go beyond or attempt to go beyond their authorised access.
    e. Managers of computer systems are required to hold a record of all access passwords in an area at all times, in a secure location.
    f. Users should log off from the network when finished at a workstation

24. 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:
    a. Where internet access is available to particular employees / persons the internet is for the College's business only. It should not be used for any private or other use. Unrelated web surfing is not permitted. Users who in the opinion of management, have abused this, will be subject to disciplinary sanction.
    b. 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.

Please note that should users wish to have sites unblocked they may do so in consultation with the ICT office.

25. Users may not bring into school an unmonitored internet connection (USB mobile plug in device etc), use any computer programs that have not been expressly permitted by the teacher or be logged into any instant messaging or social networking software while in school.

26. Students and staff will be given the opportunity to publish material to the web. The

material must not infringe on copyright. Additionally the publishing of material deemed offensive by the school will be treated as a most serious breach of discipline.

27. Material deemed inappropriate to have stored on, or accessed by digital devices used in the school includes but is not limited to: Abusive, obscene, vulgar, racist, pornographic, slanderous, hateful, threatening, sexually-orientated.

28. 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 or client machine without the expressed permission of the ICT Coordinator. This includes the use of all Web 2 tools (Web 2.0 is a loosely defined intersection of web application features that facilitate participatory information sharing, interoperability, user-centered design and collaboration on the World Wide Web see http://en.wikipedia.org/wiki/Web_2.0 for more information).

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

30. Data Storage: Where available, staff and students should save their work files on the local server according to local practice, 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.

31. Moving Data Off-site / USB Keys: Users must show due diligence when transferring, carrying and using any electronic data off the college systems e.g. working on home PCs. Coláiste Mhuire Co-Ed 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/ Laptops to transfer confidential information must be treated with great caution. The use of encrypted USB keys is necessary. Staff must not use unencrypted devices to access student data off site.

32. Personal gain or profit: Users may not use the I.T. system for unauthorised and unapproved commercial purposes or personal gain or profit.

33. Users should not subscribe to electronic services or other contracts on behalf of Coláiste Mhuire Co-Ed unless with the express authority to do so.

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

35. 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.

36. Risk of Harassment Users will not use the I.T. 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.

37. Users will not use the I.T. 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.

38. I.T. facilities should not be used to make or post indecent remarks, proposals or any material which may bring the College into disrepute. Users are advised that any form of cyber abuse against the school/ another member of the school community is not tolerated. Any incidents of cyber abuse/bullying should be reported to the Deputy Principal/Principal and will be subject to sanctions as outlined below in point 78.

39. It is not permissible to advertise or to otherwise support unauthorised or illegal activities. Users may not use the computer system for commercial purposes. This means one may not offer, provide, or purchase products or services through the computer system.

40. 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.

41. Should students cause damage to the I.T. 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:

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

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

44. 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.

45. 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.

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

47. 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.
48. 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.

In line with the draft Code of Professional Conduct for Teachers as published by the Teaching Council in 2012 teachers' attention is drawn to the following:

Article 3.3.7…*ensure that any communication with pupils/students, colleagues, parents, school management and others is appropriate, including communication via electronic media, such as e-mail, texting and social networking sites.*

Article 3.3.8…*ensure that they* [teachers] *do not access, download or otherwise have in their possession while engaged in school activities, inappropriate materials/images in electronic or other format.*

Article 3.3.9…*ensure that they* [teachers] *do not access, download or otherwise have in their possession, at any time or in any place, illegal materials/images in electronic or other format.*

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

49. Users should only use approved email accounts (eg @cmco.ie) on the school system for purposes related to their work at Coláiste Mhuire Co-Ed. If a cmco email is not available then staff are asked to set up a separate email for school business and to inform the deputy principal/principal of the details of this account.

50. Before sending internal email, consider whether this is indeed, the best form of communication to pass on the information to colleagues.

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

52. 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 I.T. team.

53. 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. Again if in doubt please consult the IT team.

54. 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.

55. 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 I.T. team immediately.

56. 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.

57. 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 the IT team.

58. To reduce the risks inherent in the The Use of the Virtual Learning Environment (Moodle)

Moodle is the virtual learning environment used by teachers and students in the school to facilitate and enhance student learning.

- Staff are encouraged to use VLEs to support and enhance the students learning.
- Staff must be aware that they should not post inappropriate material on the VLE
- Staff must be aware that quality assurance measures will be carried out on VLE content and that management can access all areas and can monitor VLE use.
- All VLE users should be aware that comments made in any of the interactive areas reflect not only on themselves but also on Coláiste Mhuire Co-Ed The VLE's communication facilities should not be used to bring the school into disrepute.
- Virtual communication and discussion are taking place in a social environment. Normal rules
- of social interaction apply and the remoteness of the recipients must not be used

as an excuse to behave in an anti-social manner and post unacceptable messages. Examples of such anti-social behaviour include:

- Harassment or intimidation of another user.
- Person to person aggression in asynchronous or synchronous communication (e.g. discussion boards or chat). Note: Synchronous commination is where online communication happens in real time. Asynchronous communication does not happen in real time.
- Any concerns regarding communication or discussion on the VLE should be brought to management immediately.
- Personal comments about other users and their views should not be placed in any synchronous or asynchronous communication areas that are viewable by other users.
- Copying private messages to another person without the author's explicit permission is a breach of confidentiality.

59. The Use of Other Technologies including Web2 applications such as Facebook.

- 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 web based I.T. program. Staff must give advance notice as it will have to go before the I.T. Committee.
- Staff should not give out their personal email addresses, Skype addresses, Facebook address or any such personal point of contact to students. This is for your own protection. If a web application has been approved by the IT Committee the staff member should set up a new account solely for educational purposes, alert the I.T. 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 Coláiste Mhuire Co-Ed 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 I.T. committee and the Principal.
- The appropriate Use of Mobile phones is governed by Code of Conduct.

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 I.T. systems, users must not

60. 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 email is confidential and may be legally privileged. It is intended solely for the addressee. Access to this email 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 email are those of the sending individual and not necessarily those of the College. It is possible for data transmitted by email to be deliberately or accidentally corrupted or intercepted.
>
> For this reason where the communication is by email, Coláiste Mhuire Co-Ed does not accept any responsibility for any breach of confidence which may arise from the use of this medium."

61. Represent yourself as someone else.

62. Forward chain emails.

63. 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

64. Perform any other inappropriate uses identified by the College.

Confidentiality

65. 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. Users 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.

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

parties.

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

68. 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.

69. Send confidential emails without applying appropriate security protocols.

Security

70. All PCs must have virus detection software installed; users must not attempt to download virus programmes themselves.

71. 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 Coláiste Mhuire Co-Ed. Staff must ensure that virus protection on personal devices is up-to-date to avoid brining viruses into the school.

72. It is essential that only software that is authorised, licenced and approved is installed on Coláiste Mhuire Co-Ed equipment, and that licence agreements are complied with.

73. Users must not intentionally interfere with the normal operation of the College I.T. 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.

74. 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.

75. Care must be taken that mobile/digital devices 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 device.

76. Care must be taken that all documents and computer media are disposed of securely at the end of their life, shredded or given to a secure digital disposal service as appropriate.

77. All computers in 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 may be asked

to assess the purposes for which the computer has been used.

Safeguarding Children

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.

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.

Protect Your Reputation, your place in school and your Career!

ADHERENCE/SANCTION.

78. It is mandatory that all personnel, students, staff, volunteers, and other users adhere to this Acceptable Use (IT) Policy. Any breach of this policy is regarded as a serious offence. Offenders shall be liable for disciplinary action, including possible termination of service, suspension or expulsion, and civil and/or criminal charges in line with the College's codes of conduct.

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

FORM OF ACCEPTANCE

I have read the Information and Communications Technology (I.T.) Resources Usage Policy of Coláiste Mhuire Co-Ed [2012] **(located at www.cmco.ie)** and confirm my acceptance and adherence to this document.

Signed: _____ Date: _____

Form Group (where applicable) _____