St John’s Central College of Further Education & Training

Quality Procedure No:	
Issue:	1.1
Applicable to:	College Staff & Students
Date/Update:	Oct 2007 Apr 2012 Feb 2013
Page:	1 of 3

Internet Policy

• Access to the Internet is provided for St. John’s Central College purposes and must not be abused for personal use.

In Brief;

- Users are expected to act ethically and responsibly in their use of the Internet / e-Mail / Social Media (such as Facebook, Twitter, YouTube, myspace.com, etc.) / and Mobile Technology (such as smartphones, tablets, etc.) to comply with the relevant national legislation, regulations and codes of practice. Users must not post messages on newsgroups or chat areas that are likely to be considered abusive, offensive or inflammatory by others.
- Discrimination, victimisation or harassment on the grounds of gender, marital status, family status, sexual orientation, religious belief, age, disability, race, colour, nationality, ethnic or national origin is against College Policy. Users must not bully, hassle or harass other individuals via Internet / e-Mail / Social Media / and Mobile Technology Users must not send messages that are likely to be considered abusive, offensive or inflammatory by the recipient/s.
- Misuse of Internet / e-Mail / Social Media / and Mobile Technology may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The College also reserves the right to report any illegal activities to the appropriate authorities.
- All security incidents involving Internet access will be reported to the IT Administrator.

Policy Detail

All users must adhere to the following when using College facilities to connect to the Internet:

• Commercial use, which is not connected to or approved by the College, is strictly prohibited and will result in disciplinary procedures,

• Users must not use the College Internet connection to scan or attack other individuals/devices/organisations. The use of port scanners or other hacking tools unless used as part of an approved course of study is strictly prohibited.

• Users should be aware that the public nature of the Internet dictates that the confidentiality and integrity of information cannot normally be relied upon.

- Where a requirement exists to send or receive confidential or commercially sensitive data over the Internet, a security mechanism recommended by the IT Administrator should be used.

- Passwords used for Internet services should not be the same or similar to passwords used for services accessed within College. This is to prevent passwords that grant access to College IT resources being sent out on the Internet in clear text where any Internet user can potentially see them. Similarly, any username used for the Internet services should not be the same or similar to a College username.

- Software copyrights and licence conditions must be observed. Only licensed files or software may be downloaded from the Internet.

- The use of the College Internet Connection to download or distribute copyright material using peer-to-peer applications is strictly prohibited. Information Systems Services reserve the right to disconnect any machines involved in illegal file distribution from the College network.

- All devices connected to the Internet must be equipped with the latest versions of anti-virus software.

- All forms of data received over the Internet should immediately be virus checked.

- All forms of data transmitted from College over the Internet should be virus checked in advance.

- Data, which has been compressed or encrypted, should be decompressed or decrypted as required before virus checking.

Wireless Internet Access Policy

- Connections of hubs, switches, routers, unapproved access points or any other device which may interfere with the campus network are not permitted. Connection sharing is not allowed. Violations will result in loss of access to the wireless network.

- Any other action that is judged detrimental to campus network operation by the IT staff may be terminated.

- The wireless connection is a direct connection to the Internet. The college does not provide virus or spyware scanning software for this connection, and therefore the risk of infections to computers increases. Connection users, not St. John’s Central College are responsible for infections originating from this wireless Internet connection.

e-Mail Policy

All users must adhere to the following when using e-Mail facilities:

- Users are expected to act ethically and responsibly in their use of e-mails and to comply with the relevant national legislation, regulations and codes of practice.

- All users should regard all e-mails sent from College facilities as first, representing the College and, secondly, representing the individual. Users should be civil and courteous. Users should not send e-mail, which portrays the College in an unprofessional light. The College is responsible for the opinions and communications of its staff and students. Any e-mail involved in a legal dispute may have to be produced as evidence in court.

- All users should do their best to ensure that email content is accurate, factual and objective especially in relation to individuals. Users should avoid subjective opinions about individuals or other organisations.

- Users should be aware that e-mails can easily be forwarded to other parties. Users should assume that anyone mentioned in e-mail could see it or hear about it or he/she may, under data protection or other law, be entitled to see it.

- All users should be aware that it is possible for the origin of an e-mail to be easily disguised and for it to appear to come from someone else.

- Users must not use a false identity in e-mails.

- Users must not create or forward advertisements, chain letters or unsolicited e-mails e.g. SPAM

- All users should protect data displayed on their monitor. This is in order to prevent unauthorised individuals from using the workstation to send an e-mail, which will appear to originate from the user.

- All users should exercise caution when providing their e-mail address to others and be aware that their e-mail address may be recorded on the Internet.

- All users should be cautious when opening e-mails and attachments from unknown sources as they may be infected with viruses.

- All users must have up-to-date anti-virus software installed and operational on the computer that they access their email on.

- All emails or attachments that are encrypted or compressed should be decrypted or decompressed and scanned for viruses by the recipient.

- Users should be aware that e-mails may be subject to audit by Information Systems Services to ensure that they meet the requirements of this policy. This applies to message content, attachments and addressees and to personal e-mails.

- As part of the College's standard computing and telecommunications practices, email systems and the systems involved in the transmission and storage of e-mail messages are normally "backed up" centrally on a routine basis for administrative purposes. The back-up process results in the copying of data, such as the content of an e-mail message, on to storage media that may be retained for periods of time and in locations unknown to the originator or recipient of an email. The frequency and retention of back-up copies vary from system to system. However, this back-up is for College administrative purposes only and it is the user's own responsibility to back-up any of their e-mails they wish to retain for future reference.

All security incidents involving E-mail should be reported to the IT Administrator.