Saint Ignatius' College

SAINT IGNATIUS' COLLEGE POLICIES

Computer Use Policy

IN PRACTICE

1. A Workplace Facility

1.1 The College's computer network is an educational and business facility provided by the College to be used primarily for educational or business purposes. College employees and students, therefore, have a responsibility to use these resources in an appropriate, ethical, professional and lawful manner.

1.2 All email and Internet based message systems on the College's system will be treated as education or business related messages.

1.3 Any information or document transmitted or stored on the College's computer network is not deemed to be private. This also applies to any medium used by employees or students within the College environment.

1.4 Workplace participants are permitted to use the College's Internet and email facilities to send and receive personal messages, provided that such use is kept to a minimum and does not interfere with the participants' responsibilities and duties in the College, or with the College's functions.

1.5 However, any use of the Internet or email for personal purposes is still subject to the same terms and conditions as otherwise described in this Policy.

1.6 Students from Years 5 – 12 have the opportunity to operate a College email account for their educational use. A contract outlining acceptable use guidelines for email use is to be signed prior to the email account being operational.

2. Appropriate Use

2.1 Individuals and/or the College may be liable for what is written or said in an email message. Email is neither private nor secret. It may be easily copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation. The audience of an inappropriate comment in an email may be unexpected and extremely widespread.

2.2 The College network, Internet or email should never be used for the following purposes:

a) to send, receive, play or store games, videos or music which are not approved for curriculum purposes;

b) to abuse, vilify, defame, harass, degrade or discriminate (by virtue of sex, race, disability, religion, national origin or other);

c) to send, receive or store obscene, offensive or pornographic material;

d) to discuss or comment on the physical appearance of another person (whether that person receives the message or not);

e) to harass any person whether through language, frequency or size of messages;

f) to injure the reputation of the College or the Church in a manner which may cause embarrassment to the employer or the Church;

g) to offend the ethos and value of Catholic teachings;

h) to spam, spoof or mass mail or to send or receive chain mail;

i) to infringe the copyright or other intellectual property rights of another person;

j) to perform any other unlawful or inappropriate act, that may be deemed by the College.

2.3 Workplace participants must not use their College email account or post messages to an Internet bulletin board, social networking site, discussion group or any other accessible discussion forum unless the message is strictly work-related or has been authorised by the Headmaster;

2.4 Excessive use of email or Internet facilities for personal reasons or inappropriate use may lead to disciplinary action including counselling, formal warnings and termination of enrolment/employment. Any employee investigations would be carried out in accordance with the "Procedures for Dealing with Allegations of Misconduct".

2.5 Any inappropriate material received by email should be deleted immediately and not forwarded to anyone else. It is particularly important to respond to inappropriate emails with an indication to the sender that such emails should not be sent in the future into, or within, the College's domain.

2.6 From time to time when accessing the World Wide Web users may be redirected to, or accidentally access, inappropriate material. These sites should be brought to the attention of the Headmaster or delegate in order for them to be blocked by the College's filtering software to ensure that it is noted that the material was not accessed purposely.

3. Network Security and Monitoring

3.1 The contents and usage of the College network, email and Internet access may be subject to regular random monitoring by the College or by a third party on the College's behalf. This will include electronic communications which are sent or received, both internally or externally. Where inappropriate use is suspected through this means, or by other incidents, the Headmaster may authorise ICT personnel to examine the web access logs and or email accounts. No monitoring will occur without the Headmaster's permission except for normal logging or system usage to manage the network. Any employee investigations would be carried out in accordance with the "Procedures for Dealing with Allegations of Misconduct".

Note: It is against College Policy for any user to attempt to:

- circumvent the security of the College network;
- bypass the Internet monitoring system used by the College.

4. Privacy

4.1 In the course of carrying out duties on behalf of the College, staff may have access to, or handle personal information relating to others, including students, colleagues, contractors, parents and suppliers. Email should not be used to disclose personal information of another person except in accordance with the College's Privacy Policy or with proper authorisation.

4.2 The Privacy Act requires individuals and the College to take reasonable steps to protect the personal information that is held from misuse and unauthorised access. When logged on, each person is responsible for the security of the computer and should not allow it to be used by an unauthorised party.

4.3 In order to comply with the College's obligations under the Privacy Act, the blind copy option should be used when sending emails to multiple recipients where disclosure of those persons' email addresses will impinge upon their privacy.

4.4 In addition to the above, users should be familiar with the National Privacy Principles ('NPPs') and ensure that the use of email does not breach the Privacy Act or the NPPs.

4.5 Because of the risk of false attribution of email, a reasonable degree of caution should be maintained regarding the identity of the sender of incoming email. The identity of the sender should be verified by other means if there are reasons for concern.

4.6 Intentionally seeking information, obtaining copies or modifying files, tapes or passwords belonging to other persons, or representing others without express authority is prohibited.

4.7 Any deliberate attempt to subvert the security facilities may incur criminal or civil liability. College employees and students are prohibited from infiltrating the system, damaging or altering software or data components of the system. Alteration to any system or network software or data component must only be undertaken if authorised by the Headmaster.

5. Distribution of Copyright

5.1 When distributing information over the College's computer network or to third parties outside the College, users must ensure that they and the College have the right to do so, and that there is no violation of the intellectual property rights of any third party.

5.2 Software must not be copied without the express permission of the copyright owner. Copyright and other laws, together with the licenses, protect most software. College employees and students must respect and abide by the terms and conditions of software use and licenses.

6. Conclusion

6.1 The terms of this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the College network, email and Internet facilities. College employees and students are encouraged to act with caution and take into account the underlying principles intended by this Policy. Advice should be sought from the Headmaster where there is a lack of clarity regarding appropriate action related to the College network, email or Internet use.

Extracted from the 2010 Information Handbook & 2010 College Diary