



# ST VINCENT'S COLLEGE

*(under the care of the Sisters of Charity)*

Established 1858

## ***Use of Electronic Facilities Policy***

This document sets out the security, administration and internal rules which you should observe when communicating electronically or using the IT facilities provided by St Vincent's College (the 'School'). You should familiarise yourself with the terms of this Policy in order to minimise potential damage to you, your colleagues, students and the School, which may arise as a result of misuse of email or Internet facilities.

This Policy applies to all teachers, employees and contractors of the School.

### **1. School Property**

- 1.1 The School is the owner of copyright in all email messages created by its employees and contractors in performing their duties.

### **2. Monitoring**

- 2.1 From time to time, the contents and usage of email may be examined by the School or by a third party on the School's behalf. This will include electronic communications which are sent to you or by you, both internally or externally.
- 2.2 You should structure your email in recognition of the fact that the School may from time to time have the need to examine its contents.
- 2.3 The School's computer network is a business and educational tool to be used primarily for business or educational purposes. You therefore have a responsibility to use these resources in an appropriate, professional and lawful manner.
- 2.4 All messages on the School's system will be treated as education or business related messages, which may be monitored. Accordingly, you should not expect that any information or document transmitted or stored on the School's computer network will be private.
- 2.5 You should also be aware that the School is able to monitor your use of the Internet, both during school or working hours and outside of those hours. This includes the sites and content that you visit and the length of time you spend using the Internet.
- 2.6 Emails will be archived by the School as it considers appropriate.

### **3. Personal Use**

- 3.1 You are permitted to use the 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 performance of your work duties.
- 3.2 However, you should bear in mind that 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.
- 3.3 In the case of shared IT facilities, you are expected to respect the needs of your colleagues and use the Internet and email in a timely and efficient manner.
- 3.4 Excessive or inappropriate use of email or Internet facilities for personal reasons during working hours may lead to disciplinary action.

### **4. Content**

- 4.1 Email correspondence should be treated in the same way as any other correspondence, such as a letter or a fax. That is, as a permanent written record which may be read by persons other than the addressee and which could result in personal or the School's liability.
- 4.2 You and/or the School may be liable for what you say 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.
- 4.3 You should never use the Internet or email for the following purposes:
- ✓ to abuse, vilify, defame, harass or discriminate (by virtue of sex, race, religion, national origin or other);
  - ✓ to send or receive obscene or pornographic material;
  - ✓ to injure the reputation of the School or in a manner that may cause embarrassment to your employer;
  - ✓ to spam or mass mail or to send or receive chain mail;
  - ✓ to infringe the copyright or other intellectual property rights of another person; or
  - ✓ to perform any other unlawful or inappropriate act.
- 4.4 Email content that may seem harmless to you may in fact be highly offensive to someone else. You should be aware, therefore, that in determining whether an email falls within any of the categories listed above, or is generally inappropriate, the School will consider the response and sensitivities of the recipient of an email rather than the intention of the sender.
- 4.5 If you receive inappropriate material by email, you should delete it immediately and not forward it to anyone else. It would be appropriate for you to discourage the sender from sending further materials of that nature.
- 4.6 Comments that are not appropriate in the workplace or school environment will also be inappropriate when sent by email. Email messages can easily be misconstrued. Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner.

- 4.7 You should be aware that use of the School's computer network in a manner inconsistent with this policy or in any other inappropriate manner, including but not limited to use for the purposes referred to in paragraph 4.3 of this policy, will give rise to disciplinary action, including termination of an employee's employment or contractor's engagement.

## **5. Privacy**

- 5.1 In the course of carrying out your duties on behalf of the School, you 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 except in accordance with the School's Privacy Policy or with proper authorisation.
- 5.2 The Privacy Act requires both you and the School to take reasonable steps to protect the personal information that is held from misuse and unauthorised access. We stress therefore, that you take responsibility for the security of your personal computer and not allow it to be used by an unauthorised party, which specifically includes anyone who is not an employee of the School.
- 5.3 You will be assigned a log-in code and you will also select a password to use the School's electronic communications facilities. You should ensure that these details are not disclosed to anyone else. We suggest that you take steps to keep these details secure. For example, you should change your password regularly and ensure that your log-in code and password are not kept in writing close to your working area.
- 5.4 You are encouraged to either lock your screen or log-out when you leave your desk. This will avoid others gaining unauthorised access to your personal information, the personal information of others and confidential information within the School.
- 5.5 In order to comply with the School's obligations under the Privacy Act, you are encouraged to use the blind copy option when sending emails to multiple recipients where disclosure of those persons' email addresses will impinge upon their privacy.
- 5.6 In addition to the above, you should familiarise yourself with the National Privacy Principles ('NPPs') and ensure that your use of email does not breach the Privacy Act or the NPPs. If you require more information on the Privacy Act and how to comply, please contact the Director of Information Technology.

## **6. Distribution and Copyright**

- 6.1 When distributing information over the School's computer network or to third parties outside the School, you must ensure that you and the School have the right to do so, and that you are not violating the intellectual property rights of any third party.
- 6.2 If you are unsure of whether you have sufficient authorisation to distribute the information, we recommend that you contact the Director of Information Technology.
- 6.3 In particular, copyright law may apply to the information you intend to distribute and must always be observed. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files and downloaded information) must not be distributed through email without specific authorisation to do so.

## **7. Encryption and Confidentiality**

- 7.1 When email is sent from the School to the network server and then on to the Internet, the email message may become public information. Encryption will reduce the risk of third parties being

able to read email and should be used in cases where you feel additional security is required. If you require more information in relation to encrypting messages, you should contact the Director of Information Technology.

- 7.2 As mentioned above, the Internet and email are insecure means of transmitting information. Therefore, items of a highly confidential or sensitive nature should not be sent via email. You should note that there is always a trail and a copy saved somewhere, not necessarily only on the School's network server.
- 7.3 This confidentiality requirement applies even when encryption is used.
- 7.4 Email sent over the Internet may be truncated, scrambled, or sent to the wrong address. There is a possibility that outgoing email sent over the Internet may arrive scrambled or truncated, may be delayed, may not arrive at all, or may be sent to the wrong address. Where outgoing email is important or urgent, you should verify that the recipient has received the email in its entirety.
- 7.5 You must ensure that all emails that are sent from your email address contain the School's standard disclaimer message, which will read as follows:
- The contents of this email are confidential. Any unauthorised use of the contents is expressly prohibited. If you have received this email in error, please advise by telephone (reverse charges) immediately and then delete/destroy the email and any printed copies. Thankyou.*  
[This message will be set to appear automatically on each outgoing email. Please contact the Director of Information Technology if this feature is not working]
- 7.6 There is a risk of false attribution of email. Software is widely available by which email messages may be edited or 'doctored' to reflect an erroneous message or sender name. The recipient may therefore be unaware that he or she is communicating with an impostor. Accordingly, you should maintain a reasonable degree of caution regarding the identity of the sender of incoming email. You should verify the identity of the sender by other means if you have concerns.
- 7.7 Please delete old or unnecessary email messages and archive only those email messages you need to keep. Retention of messages fills up large amounts of storage space on the network server and can slow down performance. You should maintain as few messages as possible in your in-boxes and out-boxes. If there are items in your email which you require at later date, please ensure that these are saved in your network directory so that appropriate backups are made School wide.

## **8. Viruses**

- 8.1 All external files and attachments must be virus checked using scanning software before they are accessed. The Internet is a potential host for computer viruses. The downloading of infected information from the Internet is potentially fatal to the School computer network.
- 8.2 A document attached to an incoming email may have an embedded virus.
- 8.3 Virus checking is done automatically through the Norton AntiVirus software installed on the College network. If you are concerned about an email attachment, or believe that it has not been automatically scanned for viruses, you should contact the Director of Information Technology.

## **9. Absence**

- 9.1 In cases where you are likely to be absent from work for any period of time, you should make arrangements for your emails to be accessible by the School or ensure that an 'out of office reply'

is automatically set. This automatic reply will alert those trying to contact you that you are away from work and that important queries should be directed to a nominated colleague. If you require assistance in installing this feature, please contact the Director of Information Technology.

## **10. Policy Updates**

- 10.1 This policy may be updated or revised from time to time. The School will not notify you each time the Policy is changed. If you are unsure whether you are reading the most current version, you should contact the Director of Information Technology.

## **11. General**

- 11.1 The terms and recommended conduct described in this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the School's email and Internet facilities. You are encouraged to act with caution and take into account the underlying principles intended by this Policy. If you feel unsure of the appropriate action relating to use of email or the Internet, you should contact the Director of Information Technology.