



# ST AGNES' PRIMARY SCHOOL

## Email & Internet 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 Agnes', Matraville. 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.

The Policy applies to all teachers, employees and contractors of the school.

### THE SCHOOL / CEO PROPERTY.

- The School/CEO is the owner of copyright in all e-mail messages and attachments created by its employees and contractors in performing their duties.

### MONITORING

- The volume of Internet traffic is tracked by schools and in CEO Offices.
- The CEO systems capture and record all Internet browsing and provide local SINA administrators with the capacity to extract historical reports for any user or user group. In particular reports may be generated that provide detail concerning any attempt to visit sites that are blocked by the filter list.
- The CEO captures and stores records of e-mail transactions across the network, including date, sender, time, recipient and size of message.
- From time to time, the contents and usage of e-mail may be examined by the School/CEO or by a third party on their behalf. This will include electronic communications, which are sent to or received by you, both internally and externally.
- E-mail messages suspected of being SPAM are forwarded to local SINA administrators who review and forward on or delete.
- E-mail is scanned for viruses and for words that would be considered offensive. If an e-mail is blocked, the SINA administrator will advise you as soon as possible.
- You should structure your e-mail in recognition of the fact that the School/CEO may from time to time have the need to examine its contents.
- The School/CEO 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.
- All messages, which may be monitored. Accordingly, you should not expect that any information or document transmitted or store on the School/CEO computer network will be private.
- You should also be aware that the School/CEO is able to monitor your use of the Online Services, 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.

### PERSONAL USE

- You are permitted to use the Internet and e-mail 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.
- Internet or e-mail for personal purposes is still subject to the same terms and conditions as otherwise described in this Policy.
- Excessive or inappropriate use of e-mail or Internet facilities for personal reasons during working hours may lead to disciplinary action.

### CONTENT

- E-mail 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 liability for you, the school and/or the CEO.
- E-mail 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 e-mail may be unexpected and extremely widespread.

- You should never use the Internet or e-mail 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/CEO 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.
- Comments that are not appropriate in the workplace or school environment will also be inappropriate when sent by e-mail. E-mail messages can easily be misconstrued. Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner.
- You should observe general courtesies when constructing emails such as addressing the recipient/s by name and concluding with a salutation.
- You should use a 'signature block' on e-mails that include your name, phone and fax number. E-mails sent from the Online Services will automatically include a Confidentiality and Disclaimer Statement.
- You should be aware that use of the School/CEO Online Services in a manner inconsistent with his policy may give rise to disciplinary action, including termination of any employee's employment or contractor's engagement.

## **PRIVACY**

- In the course of carrying out your duties on behalf of the School/CEO, you may have access to, or handle personal information relating to others, including students, colleagues, contractors, parents and suppliers. E-mails should not be used to disclose personal information of another except in accordance with the CEO Privacy Policy.
- The Privacy Act requires both you and the School/CEO to take reasonable steps to protect the personal information that is held from misuse and unauthorised access. It is therefore stressed 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.
- You will be assigned a log-in code and will also select a password to use the Online Services. You must ensure that these details are secure and not disclosed to anyone else. 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.
- 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.
- In order to comply with the obligations under the Privacy Act, you are encouraged to use the blind copy option when sending e-mails to multiple recipients where disclosure of those persons' e-mail addresses will impinge upon their privacy.

## **DISTRIBUTION AND COPYRIGHT**

- When distributing information over the Online Services or to third parties outside the School/CEO, you must ensure that you have the right to do so, and that you are not violating the intellectual property rights of any third party.
- If you are unsure of whether you have sufficient authorisation to distribute the information, you should contact your Principal/Director.
- 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 e-mail without specific authorisation to do so.

## **ENCRYPTION AND CONFIDENTIALITY**

- E-mail messages are not at this point encrypted within the CEO. Encryption is only necessary for very secure transmissions, which would most likely be transmitted across the Internet. Encryption software is to be licensed for both sender and receiver, and there are extra procedures to be followed. This statement is relevant to a very small group of staff who may install reciprocal encryption tools for communication in the future.
- There is a risk of false attribution of e-mail. Software is widely available by which e-mail 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 e-mail. You should verify the identity of the sender by other means if you have concerns.

- Please delete old or unnecessary e-mail messages and archive only those e-mail 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 e-mail which you require at later date, please ensure that these are saved in your network directory so that appropriate backups are made School wide.

## **VIRUSES**

- 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 infect information from the Internet is potentially fatal to the School/CEO computer network.
- A document attached to an incoming e-mail may have an embedded virus. If you are concerned about an e-mail attachment, or believe that it has not been automatically scanned for viruses, you should contact the ICT Helpdesk.

## **INCOMING OFFENSIVE USE OF THE ONLINE SERVICES**

- If you receive or become aware of any of the following:
  - Threatening e-mail from colleagues, students or unknown senders
  - Offensive material via e-mail or internet such as pornography and particularly child pornography.
  - Offensive remarks or threats made against you on websites or internet bulletin boards.

You should not open attachments or continue to view the material. Do not forward the material to anyone else. Immediately inform your Principal/Director and **await direction before deleting the material, as it may be required for investigation purposes.**
- Every endeavour will be made to track those responsible for sending or posting threatening e-mails or Internet messages to or about employees. Your Principal/Director will need to briefly examine the material and then immediately:
  - Contact the Head of Employment Relations or the Child Protection Officer at the CEO
  - Contact the Police in your Local Area Command (where illegal conduct has occurred)
- The Police may
  - Ask for the Internet Provider (IP) address of the sender and this can be obtained from the schools' My Internet manager.
  - Come to the school and make a copy of the material for their investigation and may wish to question employees.
  - Refer the matter to a specialised branch of the Police.

Principals and employees should always verify the bone-fides of Police when they attend the school and where possible received written requests from them before supplying data or access to equipment at the school.
- The CEO will support an investigation (in conjunction with the Police where applicable) into serious matters of harassing or threatening e-mail or Internet messages and will take whatever reasonable steps are available to prevent this occurring. **However, it is important to note that it is often impossible to determine the specific origins of e-mails and Internet messages.**

## **THE CONDUCT OF THE SINA ADMINISTRATOR**

- The SINA Administrator and Computer Operations Staff at the school/CEO may inadvertently see private and confidential information in the performance of their duties. They are not permitted to disclose or otherwise use the information.
- The SINA Administrator will routinely monitor the volume of e-mail and Internet traffic at the School/CEO and will report to the Principal/Director (or their delegate) on any suspicious activity before investigating any further.
- The Principal/Director will instruct the SINA Administrator on how to proceed.
- SINA Administrators must not independently carry out any specific viewing of suspicious material, but must be supported by the Principal/Director or their delegate.

## **POLICY UPDATES**

- This policy may be updated or revised from time to time. The School/CEO has installed a 'pop-up' reminder on the system that will alert staff to the policy at all times and will specifically mention any amendments.