Information Technology (IT), Computer, Telephone and Electronic Equipment Policy

This policy addresses issues in relation to:
Safe and Supportive Environment – Student Welfare 3.6.2

(See also Policies on Code of Conduct and Social Networking)

Purpose:

The purpose of this policy is to set out accepted uses of information technology (business and limited personal use).

1. Introduction

1.1 Application

This policy applies to the use of all school telephones, computers and electronic equipment (including use of the local or hard drive, public network, internet, e-mail, voice mail and other electronic communication technologies as well as equipment and machinery).

All employees using School Systems must comply with this policy.

1.2 Consequences of Breach of this Policy

Use of School Systems in a manner inconsistent with this policy or in any other inappropriate manner may result in the School taking whatever disciplinary action it considers appropriate. Disciplinary action may include, but is not limited to, limitation or removal of access to School Systems or termination of an employee's employment or contractor's engagement with the School.

2 Responsibilities of Staff

2.1 Accountability and Care of Equipment

Staff must use the School's equipment appropriately, and follow all instructions about how to use it and how to take care of it.

All users are issued with a unique username and password. Staff are solely accountable for all actions performed under their username and password.

Staff are accountable for:

a) damage to the School's equipment;
b) costs incurred by their access of internet sites; and/or
c) legal obligation created by their use of School Systems.

When using internet and electronic communications, staff must:

a) always identify themselves clearly and honestly;

b) not disclose to anyone passwords except as required by the School; and
c) never access another person's email or internet account without that person's permission or the permission of the School.

2.2 Viruses

All external files and attachments must be virus checked using installed scanning software before they are accessed. Virus checking is done automatically through the software installed on the mail server. If staff are concerned about an e-mail attachment, or believe that it has not been automatically scanned for viruses, staff should contact the IT Department.

Staff must not knowingly introduce a virus to the School Systems.

3 Permitted and Prohibited Uses of School Systems

3.1 Permitted Uses: Business Purposes

School Systems are a business tool and must only be used:
a) for the School's business purposes, except as otherwise set out in this Policy; and
b) in a professional, appropriate and lawful manner.

3.2 Personal and Other Uses

The School may, as a matter of discretion, allow use of School Systems for other purposes including personal use, so long as this does not:
a) contravene this Policy or other School policies; or
b) adversely impact on the performance of work duties.

The School may cease to allow such other uses at any time. Excessive use of the telephone, e-mail, internet facilities or computer systems for personal reasons may result in disciplinary action, which may include, but is not limited to, limitation or removal of access to School Systems or termination of an employee's employment or contractor's engagement with the School.

3.3 Prohibited Uses

School Systems must not knowingly be used to:
a) send or receive material that is, or may be construed to be, obscene, derogatory, defamatory, harassing, threatening, vilifying, racist, sexist, sexually explicit, pornographic, or otherwise offensive or excessively personal;

b) send or receive material which harasses or promotes hatred or discrimination based on any unlawful grounds against any person (refer to the School's Discrimination, Harassment and Bullying Statement);

c) injure the reputation of the School or cause embarrassment to the School;

d) send or receive material relating to the manufacture, use, sale or purchase of illegal drugs or dangerous materials or to any other illegal activity;

e) spam or mass mail or to send or receive chain mail;

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

g) play games;

h) game, wage or bet;

i) contribute to electronic bulletin boards;

j) perform any activity using an anonymous or misleading identity;

k) engage in any other illegal or inappropriate activity;

l) provide services or produce materials for commercial gain; or

m) access social networking sites including, but not limited to, Facebook, Twitter, MySpace and LinkedIn unless staff have been specifically authorised to do so by the Head of Campus / Executive Principal or the Head of Campus / Executive Principal's Delegate (see Social Networking Policy).

3.4 Downloading of Software

Software (licensed, shareware, freeware, evaluation or otherwise) including system, application or data files may only be downloaded using procedures approved by the IT Department.

4 Logging and Monitoring

The School notifies staff that it will carry out ongoing, intermittent monitoring of use of School Systems – including emails, internet and files (including files stored on your work computer).

The surveillance is carried out by all means available to the School which may include:

a) accessing your email account or emails;

b) accessing files;

c) accessing your work computer, storage devices or communications devices;

d) accessing records of internet usage by you (including sites and pages visited, files downloaded, video and audio files accessed and data input); and

e) use of monitoring and logging software.

The School may conduct the surveillance for any purpose – including to determine if you or any other person has, or may have, breached their obligations to the School or should be subject to disciplinary action.
Surveillance in accordance with this policy will commence on the Surveillance Date[1] .
The School may copy, access or disclose any information or files that are stored, processed or transmitted using the School's Systems.

[1] **Surveillance Date** means: if you are a new employee, the commencement date of your employment; or otherwise 14 days from the commencement date of this policy.

You should not have any expectation of privacy for any actions performed using School Systems, including personal e-mails or documents. You should also be aware that e-mails or documents might be archived by the School's management as it considers appropriate. In addition, files which you have deleted may still exist in the School's backup systems.
As part of its monitoring and logging of School Systems, the School may:

a) stop e-mails from entering or leaving its e-mail system if it believes it is appropriate to do so, e.g. if they are offensive or otherwise inappropriate, not work-related or wasteful of electronic resources (such as mass e-mailings); and/or

b) block staff access to particular internet websites.

5 Dealing with E-mails

5.1 School Property

The School is the owner of copyright over all e-mail messages created by its employees as part of their employment.

5.2 Inappropriate E-mails

Staff and/or the School may be liable for what is said in an e-mail message.

The audience of an inappropriate comment in an e-mail may be unexpected and extremely widespread; e-mail is neither private nor secret. It may easily be copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation.

If you receive e-mail which you think may be inappropriate, delete it immediately and do not forward it to anyone else.

Avoid using overly expressive punctuation and text formatting that can be construed in a negative way. Exclamation marks, capitals, underlining and font size are all examples that can be received negatively if used inappropriately.

Sarcasm is also often misconstrued in emails and should be avoided. A phone call or face-to-face meeting is often the best form of communication.

If staff receive an e-mail which they think may be inappropriate, staff should report it to the Head of Campus.

5.3 Confidentiality and Security

When an e-mail is sent from the School to the network server and then on to the internet, the e-mail message may become public information. Staff should encrypt e-mail messages which contain sensitive information before sending. If staff require additional information about encrypting messages, they should contact the School's IT Department.

Items of a highly confidential or sensitive nature should not be sent via e-mail, even with encryption. Consult the Head of Campus / Executive Principal or Head of Campus / Executive Principal's Delegate for alternate means of communication.

On occasion, e-mail may be used to correspond with recipients who are unknown or cannot be identified. Staff should ensure that they are able to identify the intended recipient, and should take care when sending or responding to such e-mail messages.

There is also 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, staff should maintain a reasonable degree of caution regarding the identity of the sender by other means if concerned.

E-mail may be truncated, scrambled, delayed, sent to the wrong address or not arrive at all. If outgoing e-mail is important or urgent, staff should verify that the recipient has received the e-mail in its entirety.

5.4 Representing the School

When sending e-mail messages for the School's business purposes, staff must ensure that:

a) any representations made are those of the School; and
b) the manner of expression used in the e-mail is consistent with the relevant business purpose and is in line with the College's Code of Conduct policy.

Comments that are not appropriate in the workplace will also be inappropriate when sent by e-mail. As noted above, e-mail messages can easily be misconstrued. Accordingly, words and attached documents should be carefully chosen and expressed in a clear and professional manner.

5.5 Disclaimer

In light of these issues, staff must ensure all e-mails that are sent from work e-mail addresses contain the School's standard disclaimer message, which reads as follows:

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. Please note that any views or opinions presented in this email are solely those of the author and do not necessarily represent those of the company. Finally, the recipient should check this email and any attachments for the presence of viruses. The company accepts no liability for any damage caused by any virus transmitted by this email.

This message is set to appear automatically on each outgoing e-mail. Please contact the IT Department if this feature is not working. Staff must not delete or amend this disclaimer.

5.6 Absences

If staff are likely to be absent from work for any lengthy period of time, they should make arrangements for their e-mails to be accessible by the School or ensure that an 'out of office reply' is automatically set.

6 Intellectual Property

When distributing information over the School Systems or to third parties outside the School, staff must ensure that they and the School have the right to do so and are not violating the intellectual property rights of any third party. This applies in the same way when copying information or downloading software.

In particular, copyright law may apply to the information staff intend to distribute or copy, 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. This material may be able to be used and copied in a limited way for research or educational purposes.

If staff are unsure whether they are permitted to distribute or copy particular information, they should contact the Head of Campus / Executive Principal or the Head of Campus / Executive Principal's Delegate.

7 Privacy

In the course of carrying out staff duties as an employee of the School, staff may have access to or handle personal information relating to others, including other co-workers, parents and students. E-mail should not be used to disclose personal information of another person except in accordance with the School's Privacy Policy or with authorisation from the Head of Campus / Executive Principal.

In order to comply with the School's obligations under privacy law, staff are encouraged to use the blind copy option when sending e-mails to multiple recipients, because disclosure of those persons' e-mail addresses may impinge upon their privacy.

8 General

8.1

The terms and prescribed conduct described in this policy are not intended to be exhaustive, nor do they anticipate every possible use of School Systems. Staff are encouraged to act with caution and to take into account the underlying principles of this policy. If staff feel unsure about what to do in particular circumstances, they should contact the Head of Campus / Executive Principal or the Head of Campus / Executive Principal's Delegate.

8.2 User Acceptance

Use of School Systems indicates agreement to comply with this policy. If staff do not comply with this policy, the School may take disciplinary action, up to and including termination of staff employment or engagement.

Revision History

Version	Policy Date	Review date of policy	Notes
1.0	January 2025	January 2027	*Amendments to this policy will be made based on updated legislative requirements or changes to school needs*