

HIGHVIEW COLLEGE

STAFF USE OF ELECTRONIC FACILITIES POLICY

Person Responsible – IT Manager



This document sets out the security, administration and internal rules that staff should observe when communicating electronically or using the IT facilities provided by Highview College. (the 'School'). You should familiarise yourself with the terms of these Guidelines 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.

These Guidelines applies to all teachers, employees and contractors of the School.

School Property

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

Monitoring

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 that are sent to you or by you, either internally or externally. 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. 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. 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. 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. Emails will be archived by the School as it considers appropriate.

Personal Use

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. 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 set of Guidelines. 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.

Content

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 that may be read by persons other than the addressee and which could result in personal or the School's liability. 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. You should never use the Internet or email for the following purposes:

- a. to abuse, vilify, defame, harass or discriminate (by virtue of sex, race, religion, national origin or other);
- b. to send or receive obscene or pornographic material;

- c. to injure the reputation of the School or in a manner that may cause embarrassment to your employer;
- d. to Spam or mass mail or to send or receive chain mail;
- e. to infringe the copyright or other intellectual property rights of another person;
or
- f. to perform any other unlawful or inappropriate act;
- g. For Social media sites/services (including but not limited to Facebook, MySpace, Twitter), staff should not have students as friends, associates, advocates or contacts. Nor should they use this as a communication medium for dealing with students and / or parents;
- h. Staff are not to include compromising photos of themselves or colleagues on social networking sites;
- i. Staff are not to give their mobile or home phone number to students.

For more information on Social media you should consult the colleges **Social Media Policy**.

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

Privacy & Passwords

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 Guidelines or with proper authorization. The Privacy Act requires both you and the School to take reasonable steps to protect the personal information that is held from misuse and unauthorized access. We stress therefore, that you take responsibility for the security of your personal computer and not allow it to be used by an unauthorized party, which specifically includes anyone who is not an employee of the School.

You will be assigned a username and you will also select a password complying with the **Password Management Policy** to use the School's electronic communications facilities.

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. In addition to the above, you should familiarize 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 Principal.

Distribution and Copyright

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. If you are unsure of

whether you have sufficient authorization to distribute the information, we recommend that you contact the Principal. 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 authorization to do so.

Encryption and Confidentiality

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 our Learning Technologies Co-ordinator. 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. This confidentiality requirement applies even when encryption is used. 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.

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.

KEEPING IMPORTANT RECORDS AND DELETING OLD RECORDS

Please keep a copy of any official correspondence you send via email on behalf of the school. The best way to do this is to print out a hard copy and file it in your own filing cabinet. Alternatively, the contents of an email could be pasted into a "Word" document and save in your own directory. On the other hand, please delete old or unnecessary email messages and archive only those personal email messages you really want 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.

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 infected information from the Internet is potentially fatal to the School computer network. A document attached to an incoming email may have an embedded virus. Virus checking is done automatically through the virus protector software installed on the network server and. If you are concerned about an email attachment, or believe that it has not been automatically scanned for viruses, you should contact a member of the IT department.

Absence

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 our Computer Technician.

Guidelines Updates

These Guidelines may be updated or revised from time to time. The School will not notify you each time the Guidelines are changed. If you are unsure whether you are reading the most current version, you should contact the Principal.

General

The terms and recommended conduct described in these Guidelines 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 Guidelines. If you feel unsure of the appropriate action relating to use of email or the internet, you should contact the Principal.

Policy designed by Daniel Smith - 2016

STAFF NOTEBOOK COMPUTER USE AGREEMENT

The provision of the Notebook computer is subject to the following terms.

1. The Notebook computer is provided on a 'use' basis and remains the property of the legal proprietors of Highview Christian Community College
2. The provision of the Notebook computer is related to current employment and could change if conditions of employment change. The Notebook computer is always the property of the school and must be supplied to the IT Manager or other authorised representative when requested, either:
 - a. in "as is" condition immediately upon request;
 - b. or, if nominated by the school with all personal files and programs removed:
 - i. within 24 hours of an official request in writing by the School, or
 - ii. not less than 24 hours prior to departure from the School subsequent to cessation of employment, or
 - iii. not less than 24 hours prior to the commencement of leave taken for the purpose of maternity, extended sickness, leave without pay or similar situations of a period of 3 weeks or longer.
 - c. Any variation to these arrangements will be solely at the discretion of the Principal, Business Manager and/or IT Manager. Failure to return the Notebook as in 2 b ii) and iii), will delay payment of final entitlements.
3. The Notebook computer will be used in accordance with all Codes of Conduct, as established by the School, or governing authority, presently, or in the future, in particular the, which includes strict compliance with the Australian Copyright Act 1968.
4. In the case of notebook hardware or software malfunction, the College IT Staff, will normally re-image the notebook and in the process erase the contents of the notebook hard drive.
 - a. Responsibility for maintaining backup copies of personal files resides with the staff member.
 - b. Installation of personal software, other than what is contained on the standard image (programs), is the responsibility of the Staff Member.
 - c. The College IT Staff cannot guarantee restoration of the files and programs back to anything other than that of a standard staff Notebook computer image. All damage and faults will be reported to college IT staff within a reasonable time to permit repair under Warranty conditions.
5. No unlicensed or illegal software may be installed onto the Notebook computer, and any single user license, that is the property of the school may not be loaded onto more than one Notebook computer at any time.
6. The School accepts no responsibility, and cannot guarantee support, for any unofficial software, data, etc. installed onto the Notebook computer.
7. Major reconfiguration of the Operating System, System Configuration and/or Installed Software, may be treated as negligence if undertaken without due care and permission of the IT department.
8. Security of the Notebook computer is at all times the responsibility of the Staff Member.

In particular, it should:

 - a. not be left in unattended offices or classrooms,
 - b. not be left in a situation so as to permit student access,
 - c. be stored in a secure, safe location when used outside school or during transportation.
 - d. Should not be left in a motor vehicle.
9. The physical safety and care of the Notebook computer also needs to be managed appropriately:
 - a. the machine must always be transported in the provided case,

- b. temperatures should be monitored as Notebooks are heat sensitive,
 - c. they are not to be used in the vicinity of food, drinks or chemicals,
 - d. they should not be cleaned with any products other than those approved by the IT department.
10. Password protection and network security must also be maintained. Staff must adhere to the **Password Management Policy** introduced to protect the integrity of the network, including password protected screensavers, password changes, remote access guidelines etc.
11. The notebook computer should be on school premises whenever the allocated staff member is scheduled to be at school.

Staff Notebook Computer Use Agreement designed by Daniel Smith - 2016

DECLARATION BY STAFF MEMBER

By accepting this agreement, the Staff Member agrees to accept responsibility to pay the School's repair and or replacement costs in the event that the Notebook computer is lost, stolen, or damaged, through that person's own negligence as determined by the college. The Staff Member agrees to pay the cost of any repair excess for loss or damage that may be caused to the Notebook computer through negligent or careless use that is outside warranty conditions and not attributable to normal wear and tear. In such instances, a Statutory Declaration stating the circumstances surrounding the loss or damage is required to be completed. Any decision concerning obligations under this Clause will be made by the Principal, Business Manager and/or Network Manager and will be based upon this Declaration.

All reference to the Notebook computer includes any hardware supplied with the Notebook computer, including but not limited to, add-in expansion cards, carry case, manuals, mouse and other School owned peripherals (if supplied).

Print Name _____

Signed _____

Date _____