Parklands Christian College

POLICIES AND PROCEDURES HANDBOOK

Section:	4 – Material Resources and Environment		
Item:	Technology	Item No:	4.90
Authorisation Date:	03/12/16	Pages:	14
Authorised by:	Board Chair		
Policy Owner:	School Board		
Revision cycle:	Low Risk – 2 years	Next review: 31/08/19	
Revised:	24/04/04 – 31/08/17		

1. PURPOSE

The purpose of this policy is to manage the appropriate use of Information, Communication and Technology services by students and employees of Parklands Christian College, and to manage the appropriate use of personal electronic devices by students at the College.

2. SCOPE

This policy applies to the following groups of people:

- Students, including those ages 18 years and over.
- Employees, including full-time, party-time, permanent, fixed-term and casual.
- Parents, contractors, volunteers and people undertaking work experience or vocational placements.

This policy applies to the management of all types of ICT services, as defined in the "Definitions" section below. It also applies on the school premises, as well as during school activities, such as excursions, camps and extracurricular activities, whenever Parklands Christian College's ICT services are utilised.

3. REFERENCES

2.26 Policy – Copyright
2.60 Policy – Privacy
3.24 Policy – Employee Code of Conduct
3.61 Policy – Student Code of Conduct
3.90 Policy – Workplace Bullying

4. DEFINITIONS

1. **ICT** – means information, communication and technology
2. **ICT services** – includes, but is not limited to IT networks, systems, facilities and devices, as defined below and includes those owned, leased or otherwise used by the school
3. **ICT facilities and devices** – includes, but is not limited to computers (including desktops, laptops, netbooks, palm and handheld devices, PDAs, tablets, eBook readers and related

devices such as monitors, keyboards and mice), telephones (including mobile phones and smart phones), removable media (such as USBs, DVDs and CDs), radios or other high frequency communication devices (including microphones), television sets, digital or analogue players and records (including DVD, Blu-Ray and video), cameras, photocopiers, fax machines, printers (and other imaging equipment such as scanners), Smartboards, projectors and screens, teleconferencing devices

4. **ICT network and systems** – electronic networks, the Internet, email, web mail, social media, fee-based web services, software, servers
5. **Personal electronic devices** – includes all types of mobile and smart phones, laptops, tablets, cameras and video recorders, hand-held game devices, music devices, USBs, PDAs, eBook readers, other palm and handheld devices and other equipment, as determined by the school, and owned by students
6. **College Records**: College records are information recorded in any form, including data in computer systems and data created, received and maintained by staff and systems in the transaction of business or the conduct of affairs and kept as evidence of such activity. College records are collated and stored according to the Parklands Christian College Privacy Policy.
7. **E-mail Messages:** an electronic mail (e-mail) message is a computer-based message sent via the communication network to one or more recipients. An e-mail message may be transmitted with one or more attachments, i.e. files containing text, graphics, images, digitised voice, digitised video or computer programs.
8. **Internet services:** Internet services include, but are not limited to chat, newsgroups, websites, games, banking, share trading, FTP (File Transfer Protocol).
9. **Intranet:** The intranet is a private network administered by the College, protected from Internet users by a firewall. The intranet can be viewed as an information utility for the College.
10. **Social Media:** Social Media may include (although it is not limited to): social networking sites; video and photo-sharing websites; blogs; wikis and online collaborations; forums, discussion boards and groups; podcasting services; online multiplayer gaming platforms; direct messaging services; geospatial tagging services.
11. **Recording:** Includes photos, videos and voice recordings

5. POLICY STATEMENT

All students and employees at Parklands Christian College carry responsibilities when they utilise ICT services as essential teaching, learning and business tools. Parklands Christian College wishes this technology to be utilised to its full capacity to provide the most valuable learning and teaching environment to the benefit of all. The College expects students and employees to demonstrate safe, lawful and ethical behaviour whenever using ICT services.

The College reserves the right to apply reasonable measures to monitor and audit any or all intranet, the Internet or e-mail activity undertaken by staff or students using College resources.

The College reserves the right to restrict employee or student access to ICT services if access and usage requirements are not met or are breached. Violations of this policy may result in disciplinary action or criminal proceedings where appropriate.

6. RESPONSIBILITIES

SCHOOL RESPONSIBILITIES

Parklands Christian College acknowledges its responsibility to:

1. Develop and implement this policy to ensure the full and safe utilisation of ICT services as essential teaching, learning and business tools within acceptable use parameters.
2. Develop and apply this policy to ensure that the use of electronic devices by students does not disrupt others or the normal routine of the school.
3. Communicate this policy to students, parents and employees.

4. Keep appropriate records, monitor and report on any issues related to breaches of this policy.
5. Encourage students, parents and employees to contribute to a healthy school culture.

EMPLOYEE RESPONSIBILITIES

Parklands Christian College employees have a responsibility to:

1. Uphold this policy via their own safe, lawful and ethical use of ICT services.
2. Take reasonable precautions to protect intranet, the Internet and e-mail information and systems against unauthorised access, illegal and inappropriate use, disclosure, modification, duplication and/or destruction.
3. Take reasonable steps to prevent and appropriately respond to any instances of inappropriate use of ICT services.
4. Provide guidance and model appropriate behaviour for the use of ICT services in the classroom.
5. Immediately advise the IT Manager or Head of School if they suspect that they have received a computer virus or if they receive a message that they suspect might be harmful.

STUDENT RESPONSIBILITIES

Parklands Christian College students have a responsibility to:

1. Uphold this policy by ensuring the appropriate use of ICT services via safe, lawful and ethical behaviour.
2. Take reasonable precautions to protect intranet, the Internet and e-mail information and systems against unauthorised access, illegal and inappropriate use, disclosure, modification, duplication and/or destruction.
3. Not use devices in a way that disrupts others or the normal routine of the school.
4. Immediately advising the IT Manager or Head of School if they suspect that they have received a computer virus or if they receive a message that is inappropriate or makes them feel uncomfortable.
5. Report any breaches of this policy to the Head of Secondary, Head of Primary, class teacher or the Student Care and Wellbeing Team.

PARENT RESPONSIBILITIES

Parklands Christian College parents have a responsibility to:

1. Read and understand, and ensure their child reads and understands, this policy before the student brings his/her electronic devices to school.
2. Ensure that all contact between students and parents during school hours occurs via the Student Services or Reception staff, and not through electronic devices. This remains the most vital and appropriate point of contact.

7. Acceptable and Unacceptable Activities

ACCEPTABLE PERSONAL ACTIVITIES FOR STAFF

Employees at Parklands Christian College are permitted to make limited use of the College's ICT services for personal purposes. Limited personal use refers to activities that are conducted for purposes other than accomplishing official or otherwise authorised activity.

Acceptable 'limited personal use' is described in the following way:

1. It is infrequent and brief
2. It does not interfere with the normal running of the school
3. It does not breach any law, regulation, standard, code or other policy or related procedure
4. It incurs only negligible additional expense, if any, to the school
5. It does not impede that employee's or any other employee's ability to do their job
6. It occurs during off-duty hours (including before and after work and during breaks) whenever possible
7. It is not for private commercial purposes or otherwise for the purpose of generating private income for the employee or another individual

ACCEPTABLE ACTIVITIES FOR STUDENTS

Acceptable activities for students are those which are conducted for educational purposes as supervised and approved by the school.

Examples of acceptable activities include, but are not limited to:

1. Undertaking assigned class work and assessments
2. Authoring text, artwork, audio and visual material
3. Conducting research
4. Communicating or collaborating with other students, teachers, parents or experts
5. Accessing online references such as dictionaries, encyclopaedias and so on
6. Research and learning through the school's e-learning environment
7. Developing appropriate literacy, numeracy, communication and information skills

UNACCEPTABLE ACTIVITIES FOR STAFF AND STUDENTS

The following activities are deemed unacceptable activities.

Accessing, downloading, distributing or publishing material:

1. Unlawful, illegal, unsafe or unethical material, including pirated material
2. Offensive messages, videos, music, pictures or other material
3. Chain letters or spam email
4. Insulting, harassing or attacking messages or other material
5. Material containing obscene or abusive language

Security:

1. Damaging ICT services, including disabling setting for virus protection, spam and filtering
2. Knowingly downloading viruses or any other program capable of breaching the school's network security
3. Altering any information or data without authorisation
4. Sharing usernames and passwords with others, or selecting obvious or easily 'crackable' passwords
5. Using another employee's or student's username or password
6. Sharing their own or others' (including other students' and employees') personal information (e.g. names, addresses, phone numbers, photos, credit card details) without permission via the Internet or email to unknown entities or for reasons other than to fulfil the educational program requirements of the school
7. Attempting to inappropriately access the school's ICT services outside of the user's authorised role and needs
8. Accessing the Internet while taking steps to disguise the user's identity
9. Connecting a private mobile device without prior approval
10. For students, engaging in unsupervised internet chats

Other:

1. Committing plagiarism or violating copyright laws
2. Using ICT services for unauthorised commercial activities such as political lobbying
3. Deliberately wasting printing and Internet resources
4. Any other activity or behaviour that could potentially damage the College's reputation

8. STUDENTS USING PERSONAL ELECTRONIC DEVICES

Parklands Christian College is committed to the fair and safe management of personal electronic devices so that the benefits of this technology can be utilised by students.

The College requires students to display courtesy, consideration and respect for others whenever they are using an electronic device. The use of electronic devices must not disrupt others or the normal routine of the school.

Students are to comply with the following rules when using their electronic devices at the College:

1. Students are required to switch electronic devices off or on to silent mode and put them out of sight during class unless expressly permitted otherwise by school staff.
2. Students may only use electronic devices before and after school and during recess and lunch breaks unless school staff have given express permission to use it at other times.
3. Students must not take electronic devices into exams, tests or other student assessments unless expressly permitted by school staff.
4. Students must not use electronic devices with a camera in any place where a camera would normally be considered inappropriate. This includes change rooms and toilets, or any situation which may cause embarrassment or discomfort to others.
5. Students must not invade the privacy of other students or employees of the school by recording (either via photo, video or voice recording) personal conversations or activities without express permission. Any recordings made with permission must not be distributed (for example, posted on a website) without express permission.
6. Students must not use an electronic device to bully or cyberbully students or school employees.
7. Students are reminded that it is a criminal offence to use an electronic device to menace, harass or offend another person and that calls, text messages and emails can be traced.
8. Students should ensure that all electronic devices are appropriately named or are otherwise identifiable by the student.
9. Students should store electronic devices safely and securely. Parklands Christian College accepts no responsibility for lost, stolen or damaged electronic devices while on school premises, at a school activity, or while travelling to and from school.
10. Students should only disclose their phone number to close friends and family.
11. Students must report any breaches of this Policy to a Head of School or the Student Care and Wellbeing team.

9. SPECIFIC PROCEDURES

STAFF USE OF DISCLAIMERS

The following disclaimer should be included at the end of the signature block of e-mail messages sent outside the College:

This message (including attachments) is intended for the addressee named above. It may also be confidential, privileged and/or subject to copyright. If you wish to forward this message to others, you must first obtain the permission of the author. If you are not the addressee named above, you must not disseminate, copy, communicate or otherwise use or take any action in reliance on this message. You understand that any privilege or confidentiality attached to this message is not waived, lost or destroyed because you have received this message in error. If you have received this message in error, please notify the sender and delete it from any computer. Unless explicitly attributed, the opinions expressed in this message do not necessarily represent the official position or opinions of Parklands Christian College. While all care has been taken, Parklands Christian College disclaims all liability for loss or damage to person or property arising from this message being infected by a computer virus or other contamination.

CAPTURING AND ACCESSING E-MAIL RECORDS

E-mail messages created, received or stored by staff in the conduct of, or in connection with College business are deemed to be private or documents within the meaning of the Libraries and Archives Act, Freedom of Information Act and Financial Management Standard.

Requirements for retaining and enabling access to e-mail messages include some legislative imperatives and the legal process.

E-mails (whether personal or business related) may be tendered in court as evidence and are subject to legal processes such as disclosure and subpoena. For more information, refer to section 95 of the Evidence Act and the Uniform Civil Procedure Rules for Supreme Court, District Courts and Magistrates Courts.

STORING AND DELETING E-MAIL MESSAGES

Appropriate record keeping of e-mail messages may be required. E-mail messages can be deleted:

1. If they are considered to be transitory messages of minor importance, once their administrative value ceases;
2. If considered to be of continuing value, once a copy has been captured in a suitable official record-keeping system.

Messages of continuing value are those records that need to be kept for any length of time, varying from a few months to many years; and those which are required for use by others, affect the work of others or are required to be held for evidential, accountability or legal reasons.

PRIVACY OF PERSONAL INFORMATION

Student and related parent personal information is confidential and can only be disseminated by authorised persons in specific circumstances, as defined in section 25(2) of the Education (General Provision) Act.

The personal affairs and details of staff should not be distributed to others without appropriate authority. Personal information is confidential, and all staff are expected to respect and safeguard all aspects of information confidentiality.

Where personal information is being distributed with authority, the security of this information should be considered in relation to 2.60 Policy – Privacy.

PRIVACY OF E-MAIL MESSAGES

Staff and students are not guaranteed privacy in relation to e-mail messages sent or received through the College IT system, whether they are business-related or personal. The reasons for this include the following:

1. E-mail is not secure unless it has been encoded or encrypted.
2. E-mail messages are hard to destroy. E-mail messages are backed up on a regular basis and can be recovered from these back-ups. The deletion of an e-mail message from the e-mail account does not remove the backed-up copy.
3. E-mail messages are logged. These logs include e-mail sender and recipient address, time of transmission and the content of the e-mail. These logs are necessary for routine maintenance and management of the e-mail service.

The College respects the right of staff to privacy, but the College reserves the right to:

1. Access staff e-mail messages, as defined in this policy.
2. Monitor, access, examine and pass on messages, as per below.

ACCESSING E-MAIL MESSAGES CREATED BY STAFF

The College may seek to gain access to staff's e-mail messages, in the same way as for paper-based material, where this is necessary to retrieve business information or for system maintenance.

In the case of system maintenance, the extent of access will not exceed the minimum essential for the performance of the maintenance function.

In the case of access to retrieve business information, the authority of the relevant manager is required before access is attempted, and the extent of access is restricted to no more than is necessary to locate and retrieve the relevant information.

Because it is a part of their official duties, a limited number of Information Technology staff have ongoing management authority to access and retrieve records created by other staff.

PERSONAL USE OF SOCIAL MEDIA

The College recognises that staff members may wish to use social media in their personal life. This policy does not intend to discourage nor unduly limit their personal expression or online activities.

However, staff should recognise the potential for damage to be caused (either directly or indirectly) to the College in certain circumstances via your personal use of social media when you can be identified as a Parklands Christian College employee. Accordingly, you should comply with this policy to ensure that the risk of such damage is minimised.

You are responsible for the content you publish in a personal capacity on any form of social media platform. When in doubt, you should seek guidance from the College on how to comply with the following obligations.

Where your comments or profile can identify you as a college employee, you must:

1. Only disclose and discuss publicly available information
2. Ensure that all content published is accurate and not misleading and complies with all relevant college policies
3. Expressly state on all postings (identifying you as a college employee) that stated views are your own and are not those of the College
4. Be polite and respectful to all people you interact with
5. Adhere to the Terms of Use of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws

You must not:

1. **Engage, communicate or interact with enrolled college students**
2. Post material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful
3. Imply that you are authorised to speak as a representative of the college, nor give the impression that the views you express are those of the college
4. Use your college email address or any college logos or insignia
5. Use the identity or likeness of another employee, contractor or another member of the college
6. Use or disclose any confidential information obtained in your capacity as an employee/contractor of the college
7. Imply you are authorised to speak on behalf of the college, or give the impression that any views you express are those of the college
8. Use your college email address or any college logos or insignia that may give the impression of official support or endorsement of your personal comment
9. Use or disclose any confidential information or personal information obtained in your capacity as an employee/contractor of the college

10. Post material that is, or might be construed as, threatening, harassing, bullying or discriminatory towards another employee/contractor of the college
11. Make any comment or post any material that might otherwise cause damage to the college's reputation or bring it into disrepute.

10. COMPLIANCE AND MONITORING

The College reserves the right to monitor any or all Internet – or Intranet – related activity and to monitor and inspect any or all e-mail messages sent or received by the college staff or students using college resources, in order to:

1. Identify inappropriate use;
2. Protect system security;
3. Maintain system performance;
4. Protect the rights and property of the college;
5. Determine compliance with State and College policy; and
6. Determine compliance with State and Federal legislation and regulation.

These compliance and monitoring activities include but are not limited to the following:

1. Access and examination of specific types of messages, e.g. large messages or messages containing executables, audio visual files, movie files, command files and/or pictures, in order to identify inappropriate use or to maintain system performance;
2. Access and examination of messages in specific circumstances, such as where and individual's message volume is high or at the peak periods of Christmas and Easter or on a random sampling basis, in order to identify inappropriate use or to maintain system performance;
3. Access, examination and referral of e-mail messages for good cause or to satisfy legal obligations, in compliance with legislative requirements and college policies. Good cause includes the need to protect system security, identify inappropriate use and protect the rights and property of the college; and
4. Introduction and use of content security software to protect staff and the college's computer network, systems and services from such things as viruses, offensive or libellous material and breaches of confidentiality.

CONSEQUENCES OF POLICY VIOLATION

1. Staff and student use of intranet, internet and e-mail services should be compliant with the principles and expectations laid out in this policy
2. Violations of this policy may result in restriction of access to intranet, Internet and/or e-mail services and may lead to disciplinary action (including dismissal) and/or action by the relevant regulatory authorities
3. Staff or students who are aware of or observe a suspected violation of this policy are responsible for reporting the incident to their supervisor.

11. APPROVAL

This policy was approved by the Board of the Parklands Christian College at its meeting held on _____.

Signed:	..... Chairperson		..... Secretary
Name:	.....	Name:	.....
Date:	.....	Date:	.....

12. APPENDIX

In this section:

1. Electronic Mail Etiquette
2. Effective Use of E-mail
3. Use of Attachments
4. Use of To. CC and BCC
5. Use of Distribution Lists
6. Signature Block
7. Inappropriate Internet Sites
8. Spam Mail
9. Chain Letter
10. Defamation and Harassment
11. Document and Record Management Requirements

1. ELECTRONIC MAIL ETIQUETTE

The use of appropriate etiquette in e-mail correspondence will make e-mail a more effective communication tool and will be appreciated by recipients.

Think before you write

Before you create and send an e-mail message, consider the following:

1. Is e-mail the best medium for your message? E-mail is impersonal; without facial expressions and body language to provide clues, e-mail can be misunderstood.
2. Are you overusing e-mail? Don't let e-mail replace all personal contact.
3. Consider the recipient's needs. If they do not need the information, you will be saving them time by not sending the message.
4. Is this a college 'business transaction' which is likely to make this e-mail and any subsequent e-mails college records? If so, how do I ensure their capture into the college record-keeping system?
5. Is e-mail a suitable form of communication, i.e. if highly confidential should the message be sent by e-mail?

Style points

1. Maintain professionalism.
2. Be succinct. The most effective e-mail messages are short and to the point, but not so short as to be rude.
3. Don't 'shout' by using upper case to emphasise a point you feel strongly about. This can set a negative tone.
4. Keep the message focused on a single topic. Too many topics can confuse.
5. Make it obvious what the e-mail is about. State early on why the information is being sent, what is expected of the recipient/s and when the sender would like action, if any, to be taken.
6. Appearance matters. Don't be sloppy or careless. Depending on the context, use of all lower case letters or omitting punctuation may be interpreted as laziness or lack of respect for your reader/s.
7. Consider message format. There is no guarantee that the user's e-mail facility will display the message as intended. Do not depend on alignments, fonts and colours to make a point.
8. Be courteous; don't forget please and thank you.

Good Sender Habits

1. Enter a meaningful subject that captures the content of the message. Replace vague subject lines with meaningful information; this helps recipients prioritise, file and search for messages.
2. Use distribution lists with caution. Send e-mail messages only to recipients who need the information.
3. Tag messages appropriately. Do not tag messages as 'High Priority' or 'Urgent' if they are not.

4. Do not 'reply to all' unless they all need to see your reply.
5. Do not modify someone else's message.
6. Address e-mail according to the expected action. A person listed in the 'To' field is expected to respond; one in the 'CC' field is expected to read the message as information only.
7. Before you forward messages to others, consider the need to obtain the permission of the author. For example, consider the questions: Is the forwarding of the message compliant with the author's intended use of the information? Are you forwarding the message within your work group?
8. Choose the number and size of file attachments with care and avoid trivial attachments.
9. Use graphics or pictures judiciously. Graphics or pictures as inserts do attract attention but use them sparingly as they add to the size of the e-mail message, the time it will take to deliver the message and the load on the network.
10. Review before sending. Proofread your correspondence and use the spell checker; too many mistakes can make you look careless and can damage your professional reputation.
11. Do not create or forward unsolicited e-mail, e.g. chain letters.
12. If the e-mail is a corporate record, print out a hard copy and file using the appropriate recordkeeping system.

Good Recipient Habits

1. Check your e-mail at regular intervals.
2. Use auto-replies or delegate authority when unable to check e-mail.
3. Browse the subject line or preview panel to identify important messages.
4. File important messages into organised folders.
5. Use inbox rules and filters to file messages automatically to relevant folders.
6. Think before you reply. Many communications need no reply at all. Don't reply unless you have something significant and well considered to communicate.
7. Reply or acknowledge receipt of messages promptly if the sender is expecting a response.
8. Ask to be removed from unwanted distribution lists.
9. Virus-scan attachments on e-mails received from external sources.
10. E-mails sent to external recipients may have the standard disclaimer at the end of the signature block.
11. Delete junk mail.
12. Print out and/or file college records and other important messages. The appropriate repository for filing will depend on your location and the task or subject to which this message relates.
13. Delete messages that are no longer needed.

2. EFFECTIVE USE OF E-MAIL

E-mail enables staff to send messages to others both inside and outside the department. It is important for all staff to consider the implications of sending e-mail messages to people who do not need them. The practice clogs mailboxes with unnecessary messages and wastes resources; ultimately it ends up impeding the communication system instead of enhancing it.

3. USE OF ATTACHMENTS

Use attachments sparingly. Unnecessary use of attachments is a waste of space.

Before you attach documents to an email message consider providing the recipient with either:

1. Extracts of the relevant sections of the document rather than the whole document;
2. A printed copy of the document or appropriate sections;
3. The location of the document on the network.

4. USE OF TO, CC AND BCC

1. Staff are advised to limit the number of recipients for an e-mail message. Sending a message to a very large number of recipients can congest the network; if it is necessary, consider sending separate messages to smaller groups.

2. The e-mail service makes it possible to send information to more people faster than traditional communication methods. Just because it is faster does not mean it should be done; staff need to consider who actually needs to receive their message. Sending messages to recipients who do not need them is a waste of their time and system resources. As a guide, consider whether you would make a telephone call to all potential recipients of this message.
3. Staff need to consider the intellectual property rights of authors before they forward messages to others. It is acceptable to send or forward college information to others within the college where it is relevant to their professional duties. Permission should be obtained from the author before sending or forwarding:
    a. Messages (including attachments) received from external sources;
    b. Messages (including attachments) outside the college.

5. USE OF DISTRIBUTION LISTS

1. When staff have a recurring need to communicate with a defined group of other staff, that staff member can set up a distribution list identifying all the members of the group. After that, the staff member need only address messages to the group via the use of the distribution list; the e-mail system sends the message to each member.
2. There has been a large number of distribution lists created to ease communication to groups.
3. Exercise care when using distribution lists as they can become outdated. Use of outdated distribution lists can waste time and resources.

6. SIGNATURE BLOCK

Staff may attach a signature block, containing the following minimum details, to every e-mail message sent outside the college:

1. Name
2. Position
3. Work Unit
4. Full name of the college
5. E-mail address
6. Work phone and fax
7. The signature block for e-mail messages sent within the college is at the staff member's discretion.

7. INAPPROPRIATE INTERNET SITES

Occasionally, Staff can accidentally access inappropriate websites. Staff who do so should note the date and time, leave the site and notify their supervisor, in case monitoring highlights the access and a query is raised. Supervisors can forward the inappropriate site details to their relevant technical support area to have the site blocked.

8. SPAM MAIL

1. Spam mail is electronic junk mail, and staff are receiving it in increasing quantities. In general, senders of spam mail have two purposes:
    a. To encourage recipients to purchase goods or services from the sender; and
    b. To gather live e-mail addresses for future use or on-selling.
2. Staff are requested not to respond to spam email, even when the message provides an e-mail address for you to request your e-mail address to be removed from their lists. By responding you are confirming that the e-mail address is live and the result will be an increase in the amount of spam mail received.
3. In some cases, spam email requests that the recipient visit a website, which may be a commercial site but could equally be an inappropriate site. In either case, the site will most likely have technology in place to gather identifying information about those who visit the site. It will almost invariably request that you provide personal details about yourself.
4. Spam mail increases transmission costs and takes up space in e-mail accounts. Therefore nothing should be done to encourage receipt of this type of email.

5. If you are receiving large volumes of spam email or spam mail that offers goods or services that are illegal, contact the IT Coordinator for assistance.

9. CHAIN LETTERS

1. A chain letter is a communication which includes an incentive to forward it on to others. This incentive takes the form of a promise of reward and/or a threat.
2. Forwarding of chain letters is defined as an improper communication and therefore an inappropriate use of e-mail services. Forwarding or sending of improper communications is a waste of college resources and may expose the college to the risk of legal action or adverse publicity.
3. Improper communications are in breach of the Code of Conduct and may be in violation of the law. As such they are prohibited by the college.
4. All chain letters should be deleted. If you are receiving large numbers of chain letters, contact IT Coordinator.

10. DEFAMATION AND HARASSMENT

1. Distribution of defamatory or harassing messages is an inappropriate, and improper use of e-mail services. All staff should take care constructing the content of e-mail messages to avoid potential claims of defamation, harassment or discrimination.
2. Harassment can take a number of forms including that based on gender, ethnicity, and religious and political beliefs. Harassing messages may leave the sender and/or the college liable under anti-discrimination laws and could lead to disciplinary action against the sender.
3. A statement is defamatory when its effect may be to destroy the personal or business reputation of another. Material can defame through use of words, pictures, a combination of these, or by innuendo. In some circumstances, defamation is a criminal offence.
4. Staff should also be aware of the effect that messages have on the reputation of the college. As a rule of thumb, when previewing e-mail messages, staff should read the contents of the message as though they were liable to be publicly broadcast.
5. If you have received or have inadvertently sent a message that is or could be considered to be defamatory or harassing, contact the IT Coordinator for assistance.

11. DOCUMENT AND RECORD MANAGEMENT REQUIREMENTS

1. Every staff member is responsible for ensuring electronic records/documents of continuing value are placed in the appropriate record-keeping system for future retrieval.
2. It is the responsibility of authors of internal e-mail messages and recipients of external e-mail messages to determine whether the message is of continuing value and to take appropriate action. The following lists will assist you in determining whether a message is of continuing value, but this list is not exhaustive.
3. Examples of documents of continuing value include:
    a. Any document that relates to the conduct of college business;
    b. Approvals to undertake actions relating to college business;
    c. Formal communications between staff within the college, other schools, with external organisations and members of the public,
    d. Formal minutes of meetings and committees;
    e. Final versions of reports;
    f. Amended versions of reports where instructions have been given;
    g. Policy documents; and
    h. Advice given which may influence another person's actions about college business.
4. Documents not considered to be of continuing value include:
    a. Personal messages not related to college business;
    b. Documents that do not relate directly to business;
    c. Duplicated material, e.g. an information-only copy of a document;
    d. Information distributed to a number of people, e.g. circulars, meeting agendas;
    e. Drafts of reports or correspondence;

f. Transitory of minor importance (e.g. telephone messages) which do not relate to college business;
g. Messages which perform a similar function to an informal telephone call; and
h. Unsolicited messages seeking employment or offering goods or services to the college.

5. Electronic messages may be deleted if considered to be records of continuing value once a copy has been forwarded to the relevant official record-keeping system. Electronic messages may be deleted if considered to be transitory messages of minor importance once their administrative value ceases.