NEWCASTLE GRAMMAR SCHOOL
POLICY DOCUMENT

Policy Number (PN): 14.43
Policy Name: Use of Electronic Facilities
Version: 1.1
Last Revised: October, 2008
Signed Off: Reg Yates Date: 22/07/09
Endorsed: Date: 22/7/09
Policy No.: 14.43

Name of Policy: Use of Electronic Facilities

Policy:
The policy is to ensure the safe, secure and reasonable use of the IT facilities by staff, students and visitors and supplied by NGS. NGS is an educational institution and therefore the School is the owner of copyright in all email messages created by its employees and contractors in performing their duties. All staff should be aware of the procedures listed below. This Policy should be read in conjunction with other School Policies.

Procedures:

This document sets out the security, administration and internal rules which you should observe when communicating electronically or using the Information Technology facilities provided by Newcastle Grammar School (the 'School'). This Policy applies to all teachers, employees, temporaries and contractors of Newcastle Grammar School.

General Use and Ownership
- While the School's network administration desires to provide a reasonable level of privacy, users should be aware that data they create, or emails sent and received, on the schools systems remains the property of Newcastle Grammar School. Because of the need to protect the School's network, management cannot guarantee the confidentiality of information stored on any piece of equipment supplied by the school, for use by the staff, students, or contractors.

- The School is the owner of copyright in all email messages created by its employees and contractors in performing their duties.
- For security and network maintenance purposes, authorised individuals with the School can monitor computer usage, equipment, systems and network traffic at any time. The School reserves the right to audit networks, computer systems and usage on a periodic basis to ensure compliance with this policy.

Electronic Access Privileges
- Privileges to access the School’s computing systems are tailored to individual needs and responsibilities and are assigned via a unique user logon. Authentication is required at the time of access through the use of a logon / password combination. You should ensure that these details are not disclosed to anyone else.
- To keep these details secure, staff should change their password regularly and ensure that their user log-on and password are not kept in writing close to your working area.
- The School has provided a user logon to access only information, that is publicly available or to which you have been given authorised access.
- Staff members are responsible for all activities on their user logon or that originate for computer systems which they are logged into.
- 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.
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 Policy.
- Staff are responsible for exercising good judgment regarding the personal use of the information systems, and to ensure it does not interfere with the performance of their work duties.
- Excessive or inappropriate use of the electronic facilities for personal reasons during the working hours may lead to disciplinary actions.

Privacy

- 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.
- 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.
- 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 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 Headmaster.

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 authorisation to distribute the information, we recommend that you contact the Headmaster.
- 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.

Email Systems:

Legal Risks

- Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communications, such as a letter or
facsimile, the same laws apply. Therefore it is important that users are aware of the legal risks of email.

- If you send or forward emails with any libelous, defamatory, offensive, racist or obscene remarks, you and the School can be held liable.
- If you unlawfully forward confidential information, you and the school can be held liable.
- If you unlawfully forward or copy messages without permission, you and the school can be held for copyright infringement.
- If you send an attachment that contains a virus or other malware, you and the School can be held liable.
- If you disguise or attempt to disguise your identity when sending email, or send email messages using another person’s email account, you and the School can be held liable.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules set out in this policy, the user may be solely liable for any legal action that may arise.

Confidential Information

- Never send any confidential information via email. If you are in doubt as to whether to send certain information via email, check this with the Headmaster.
- The internet and email are insecure means of transmitting information, and there is always a message trail and a copy saved somewhere and not necessarily only on the School’s server.

Password Protection

- The use of passwords to secure specific files should not provide users with an expectation of privacy in the respective systems or documents.

Encryption

- Encryption will reduce the risk of third parties being able to read email. Users may not encrypt any email without obtaining permission from the IT Department. If approved, the encryption key(s) must be made known to the IT Department or an authorised individual of the School.

Email Retention

- All email will be backed up during the School’s normal data backup procedure, see Policy Number 14.72.
- The maximum size of the email boxes is 1.5 Gb in size, it is recommended that regular cleanup of the email is conducted. The deleted items should not be used to store email.
- 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.
- Emails will be archived by the School as it considers appropriate.

System 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 which are sent to you or by you, both 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 following excerpt is taken from the Privacy Laws, Section 20-300 Employee use of E-mail and Internet.

As a general principle, employers can log all employee movements on the work email system (including e-mail addresses to which messages are sent, websites visited, times of access and transmissions) and gain access to the content of e-mails (even if deleted). An employer does not have to seek the consent of their employees to be able to monitor and access such communications and transactions, because the employer’s computers and computer systems are recognized as their property over which they can consequently exert control.

Disclaimer
• The school’s standard disclaimer will be added to each outgoing email
  o The contents of this email are confidential. Any unauthorised use of the contents is expressly prohibited. If you receive this email in error, please advise by telephone immediately and then delete/destroy the email and any printed copies. Any views expressed in this message are those of the individual sender and may not necessarily reflect the views of Newcastle Grammar School. Email communication through the Newcastle Grammar School network is monitored
  Thank you
  Newcastle Grammar School
  Newcastle, NSW Australia
  02 49295811

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 Sophos antivirus installed on the mail server and each client machines.
• If you are concerned about an email attachment, or believe that it has not been automatically scanned for viruses, you should contact 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 the IT department.

Internet Access:

System Monitoring
• From time to time, the usage of the internet may be examined by the School or by a third party on the School’s behalf.
• Internet usage is logged through both the use of the proxy server logs and the access logs from the firewall
• Computer realtime monitoring may be used to ensure compliance with this policy, and to log current activity while being monitored.

Unacceptable Use:
The following activities are, in general prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., IT Support staff, Headmaster). Under no circumstances is an employee or student of the School, or visitors to the School authorized to engage in any activity that is illegal under local, state, federal and international law while utilizing the School-owned resources.

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the School.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the School or the end user does not have an active license is strictly prohibited.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using the School's computing assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any School e-mail account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to IT Department is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, School employees, parents or students to parties outside Newcastle Grammar School.

Best Practices
The School considers email as an important means of communication and recognises the importance of proper email content and appropriate replies in conveying a professional
image and delivering good communications. Users should take the same care in drafting an email as they would for any other communication.

Guidelines for writing emails:

- Write well-structured emails and use short, descriptive subjects.
- Emails are often informal. This means that sentences can be short and to the point. You can start your email with ‘Hi’, or ‘Dear’, or ‘Good Morning’, etc, and the name of the person. Messages can be ended with ‘Best Regards’. The use of Internet abbreviations and characters such as smileys however, is not encouraged.
- Outgoing emails must include your name, job title and company name. A disclaimer will be added underneath your signature (see Disclaimer).
- Users must spell check all mails prior to transmission.
- Do not send unnecessary attachments. Compress attachments larger than 200K before sending them.
- Do not write emails in capitals.
- Do not use cc: fields unless the cc: recipient is aware that you will be copying a mail to him/her and knows what action, if any, to take.
- The only acceptable use for the bcc: field is when a bulk email is required to be sent to many people, and you do not want all the other recipients to see it, in accordance with the privacy laws. Do not use bcc: fields as the recipient is unaware that you will be copying a mail sent to him/her to someone else, and the recipient does not have the opportunity to reply to the other person.
- If you forward emails, state clearly what action you expect the recipient to take.
- Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password (see confidential).
- Only mark emails as important if they really are important.

Replying to emails

- Emails should be acknowledged within 24 working hours, but users must endeavor to acknowledge priority emails by the end of the working day.
- Emails which are received after 5pm should not be replied to until after 10AM the next day unless it is extremely urgent or matter of fact.
- Internal emails are to be replied to as necessary
- Emails from parents are to be replied to within 24 hours.
- External emails are to be replied to as is appropriate.

Newsgroups

- Users need to request permission from the IT Department and your Faculty Head before subscribing to a newsletter or news group.

Maintenance

- Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your ‘deleted items’ on closing.

Content
• 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:
  - 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.
• 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.

Encryption and Confidentiality
• 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.

Policy Updates
• 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 Headmaster, or review the latest School policies on the School's intranet.

General
• 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 Headmaster.