USE OF COMMUNICATION AND INFORMATION TECHNOLOGY DEVICES

PREFACE

We aim to be an effective organisation. The implementation of best practice management systems that foster a cooperative and productive workplace and ensure the effective use of available resources is one way of achieving this. As a public sector agency, we must be efficient, economical and ethical in our use and management of public resources provided for business purposes, including devices such as telephones, email, USB drives and PDA’s.

PURPOSE

This policy sets out the responsibilities of staff when using communication and information technology devices, informs staff of the systems in place to monitor use of communication and information technology devices, addresses certain security issues and provides guidance on the status of emails as official records of our business activities.

RESPONSIBILITY

This policy applies to the Ombudsman and all staff of the office, whether by way of appointment, secondment, contract, temporary arrangement or on a fee-for-service basis. Any individual having employee functions or acting in an employee capacity, or engaged by the Ombudsman including a volunteer, is a member of staff for the purpose of this policy.

The Security and Information Management Steering Committee or Director Corporate may make procedures, templates or guidelines supporting this policy. Staff will also be bound by these.

LEGISLATIVE/POLICY FRAMEWORK

Ombudsman Act 1974
Workplace Surveillance Act 2005
State Records Act 1998
Department of Premier and Cabinet, Policy and Guidelines for the use by Staff of Employer Communications

This policy supersedes the Use of Communication and Information Technology Devices Policy dated 16 January 2006.
DEFINITIONS

*Communication or information technology device* includes, but is not restricted to the following devices:

- **Camera** includes an electronic device capable of monitoring or recording visual images of activities on premises or in any other place.
- **Computers** include, but are not limited to, desktop computers, servers connected to our network or office owned portable (laptop) computers.
- **Electronic data interchange** or electronic document interchange refers to the application-to-application exchange of computer-based information over a data circuit.
- **Email** (also known as electronic mail) refers to a computer-based message sent over a communications network to one or more recipients. It may be transmitted with attachments such as electronic files containing text, graphics, images, digitised voice, digitised video or computer programs.
- **Facsimile** refers to a communication device that converts each picture element of black and white into an electric signal. These signals in turn generate a constantly changing electrical signal that is transmitted on a data circuit (or telephone line) to a receiving facsimile.
- **Internet** is a world-wide loose affiliation of interconnected computer systems (involving government, commercial, academic and hobby providers) through which an individual with a personal computer can access services and information. Services available through the internet include, but are not necessarily confined to, electronic mail, Telnet and the World Wide Web (www).
- **Intranet** is an internal (restricted) network that uses internet technology. It is accessed over a personal computer.
- **Pager** refers to a small telecommunications device that receives (and in some case sends) short radio messages (either numeric or alphanumeric) and is generally used by people who are continually changing their location. When a pager captures a message it is usually accompanied by a beep to alert the person carrying the pager. Also known as a ‘beeper’.
- **PDA** (personal digital assistant) refers to a handheld computer that serves as a mobile organiser and allows data such as email, outlook calendar appointments and contacts to be accessible while away from the desk. Data is synchronised between the PDA and desktop computer via a synchrony cradle. Only PDA’s authorised by the office may be used on the office network. Staff must comply with procedures supporting this policy when using an office PDA.
- **Radio** refers to wireless electromagnetic means of point to many point communications.
- **Telephones** include, but are not limited to, hard-wired desk telephones, cordless telephones and mobile (cellular) telephones.
- **USB drive** refers to a small, portable flash memory stick that plugs into any computer’s USB port and functions as a portable hard drive. A USB drive is small enough to be carried in a pocket and allows data to be easily transferred from one machine to another. Only USB drives authorised by the office may be used on the office network. Staff must comply with procedures supporting this policy when using an office USB drive.

POLICY STATEMENT

1. **Access to communication and information technology devices**

All access to communication and information technology devices owned or used by the Ombudsman is subject to this policy. Only staff who have signed a written undertaking that they have read, understand and will abide by this policy will have access to office communication and information technology devices.

Access to the office’s internet service provider accounts must only be through authorised office equipment located in the office.

Staff may only use an office mobile telephone if it has been allocated to them by the Ombudsman, a statutory officer or division manager as necessary to perform their job, or in accordance with the specified procedures.

Staff may only access an office laptop computer in accordance with the specified procedures.
2. Monitoring of use

Communication and information technology devices are provided by the office for work-related purposes. While reasonable private use is authorised (please see the section in this policy on economic use), personal use of these devices will be subject to the same level of scrutiny as work-related use.

All information, data or files created by you while employed by the office are subject to scrutiny. Electronic messages are official documents that are subject to the same laws as any other form of correspondence.

The office may monitor, copy, access or disclose any information or files that are stored, processed or transmitted using office equipment and services. The office may monitor email and internet use by staff on a random or continuous basis to:

- prevent the downloading of unauthorised software
- ensure compliance with office policies
- investigate conduct that may be illegal or adversely affect the office or our staff, and
- prevent inappropriate or excessive personal use of office property.

Email filtering is necessary to protect the office computer network from constant threats such as viruses and spam. All inbound emails are monitored automatically by software. Emails determined to be spam, to contain viruses or files that are potentially dangerous to internal networks are blocked. IT staff manually check blocked emails to determine their appropriateness for release. Employees will be notified of blocked emails unless they are believed to be spam or to contain viruses. IT staff must comply with procedures supporting this policy when monitoring and releasing blocked emails.

Staff internet use is monitored automatically by software. Each website is pre-scanned to determine if it contains pornography, otherwise offensive material or content dangerous to internal networks. In addition, the software continually monitors staff internet use which is then used to conduct periodic random audits. The office may conduct ad-hoc audits of individual staff at the request of a statutory officer or division manager. Audits include reviewing visits to offensive and inappropriate sites, and whether levels of personal internet use are inappropriate. There is a monthly review of all staff internet usage.

All inbound and outbound telephone calls are monitored continually by software. Reports may be used to isolate or identify problems with the switchboard, or to identify or monitor abusive or inappropriate calls. Reports may also be used at the request of individual staff to identify personal calls for the purposes of staff contribution.

Supervisors intermittently monitor inquiries staff work-related telephone calls for induction and training purposes. This is only done with the staff member’s knowledge.

Any calls that are made on an office mobile telephone will be recorded on the telephone bill. Mobile telephone expenditure must be reviewed and approved by a division manager or a statutory officer.

3. Economic use

Computer equipped workstations and the services accessible on them, mobile telephones, portable computers, PDA’s and USB drives are provided to staff for business use. Reasonable private use of the internet, email, telephones is a privilege and needs to be balanced in terms of the office’s commitment to having a responsive and flexible workforce, and ongoing operational needs.

(a) Telephones

Where possible and appropriate, staff are encouraged to use free-call telephone services. These generally provide more economical and efficient means of communication. Because all calls involving a mobile telephone are time charged, staff members should keep short any communication involving a mobile telephone. This applies equally to calls made from standard desk telephones as well as calls from mobile telephones. Calls involving mobile telephones should be avoided where standard desk telephones are readily available.
(b) Email

While email may be used for official communication purposes, you should continue to send written correspondence by post where this would be ordinary procedure. Email may be used where it is the requested form of communication by external parties and/or where the efficiency of inquiries, investigations or other business would be facilitated by the use of email.

Any communication sent by email should also be in accordance with general office procedures (including the email protocols included at Annexure A), your level of delegation for the sending and signing of correspondence and any supervision approval requirements that apply.

(c) Internet

All internet use must have a clearly defined purpose at the outset of any session. If you are accessing the internet from a standalone computer, you must remember to log off before leaving the workstation. Try to avoid leaving unnecessary internet applications open when not in use, as this can add to your internet usage figures. You should be mindful that standalone computers are a resource to be shared with other staff members and use them only for as long as necessary.

4. Lawful and ethical use

Staff must not intentionally create, send or access information that could damage the reputation of the office, be misleading or deceptive, result in victimisation or harassment, lead to criminal penalty or civil liability, or be reasonably found to be offensive, obscene, threatening, abusive or defamatory.

Inappropriate use includes, but is not limited to, any use of equipment or services of the office for intentionally transmitting, communicating or accessing pornographic or sexually explicit material, images, text or other offensive material.

If you receive and open an email that contains pornographic or sexually explicit material, images, text or other offensive material, you must immediately:

- forward the email to the Director Corporate, who has responsibility for monitoring email and internet use by staff
- reply to the sender of the email indicating that the material is inappropriate, that the message will be deleted and that no further communications of a similar nature should be sent to you
- delete the email from your Inbox, Sent Items and Deleted Items.

It is inappropriate to transmit, communicate or access any material, which may discriminate against, harass or vilify any person with whom you have business dealings, including a colleague or any member of the public.

In particular, it is unlawful to do this on the grounds of the person’s:
- race (including colour, nationality, descent or ethnic background)
- sex
- disability
- age
- homosexuality
- marital status
- pregnancy
- identification as a transgender person
- identification as a carer
- having HIV/AIDS.

In addition, it is inappropriate to transmit, communicate or access any material that may discriminate against, harass or vilify any person with whom you have business dealings on the grounds of political or religious conviction.
You may be individually liable if you help others who discriminate against, harass or vilify colleagues or any member of the public. (Harassment will be treated in accordance with the grievance and dispute management policy and may result in disciplinary action).

Staff must not intentionally create, transmit, distribute, or store any offensive information, data or material that violates Australian or State regulations or laws. The office reserves the right to audit and remove any illegal material from its computer resources without notice.

The use of any telecommunications system to make or send fraudulent, unlawful, or abusive information, calls or messages is prohibited. Staff who receive any threatening, intimidating or harassing telephone calls or electronic messages should immediately report the incident to their supervisor and their statutory officer. Any staff member who initiates fraudulent, unlawful or abusive calls or messages may be subject to disciplinary action and possible criminal prosecution.

The use of a hand held mobile telephone while driving is an offence under Australian Road Rules and the office will not be responsible for the payment of any fines.

No form of computer hacking (illegally accessing other computers) is allowed. Any such behaviour may result in disciplinary action and possible criminal prosecution.

5. Accessing certain websites
Where a genuine business reason exists that requires access to websites that would be normally regarded as inappropriate, the written authorisation of a statutory officer or the Director Corporate is required. This should be forwarded to the Security and Information Management Steering Committee.

6. Personal use
The Ombudsman is committed to having a responsive and flexible workforce and acknowledges that family and community responsibilities impact on work. In implementing flexible work practices and other relevant policies of the NSW public sector, the office recognises that its communication and information technology devices may need to be used for personal reasons. Such use should be infrequent and brief, and should not involve activities that might be questionable, controversial or offensive. This includes, but is not limited to:

- gambling
- accessing chat lines
- transmitting inappropriate jokes
- subscribing to lists, newsgroups or chat groups
- sending junk programs or mail, or
- intentionally downloading unauthorised software or lengthy files containing picture images, and live pictures or graphics, including computer games, music files and the accessing of radio or television stations broadcasting via the internet.

Personal use does not extend to the sending of non-business related written material to any political organisation.

Personal use of office communication and information technology devices is not considered private, and members of staff using such devices do not have the same personal privacy rights as they would have when using private or public (eg. coin or card operated telephone) communication and information technology devices. Staff reasonably suspected of abusing personal use of office communication or information technology devices may be asked to explain such use (which may be monitored as part of the Ombudsman’s responsibility to implement appropriate control mechanisms).
7. Record keeping

Business communications that are sent electronically (eg. email messages) become official records, subject to statutory record keeping requirements. Subject to the exclusions contained in the Ombudsman Act, they can also be subpoenaed or 'discovered' during legal processes. Business communications sent electronically must be maintained in an electronic form and a hard copy is to be made and placed on the official file. The electronic version is to be filed into the appropriate context folder and can then be deleted from your mailbox.

You should regularly empty your inbox of superfluous emails that have been alternatively stored.

If your supervisor agrees that the bulk and relevance of email attachments is such that it would be an unreasonable use of resources to print hard copies to be attached to the relevant file, the email and attachments should be saved electronically into the appropriate context file and a notation put on the relevant hard copy file.

8. Security

Members of staff should always be aware that any messages conveyed through communication and information technology devices can be intercepted, traced or recorded by others. Although such practices are usually illegal, you should not have an expectation of privacy. Password or personal identity number protection should be used on all mobile devices (eg. mobile telephones, laptop computers, PDA’s and USB drives) that are vulnerable to theft. You must take due care with all communications and the sending of confidential documents. You must exercise caution when entering into any on-line purchasing arrangements. As with telephone orders, you must first obtain proper authorisation for purchases.

Email is not be used to send Highly Protected or Protected documents unless there are special circumstances and approval of a statutory officer or Director Corporate is given (see the Information Security Policy).

The use of your computer is monitored through a 'user id' and access rights governed by a password personal to you. Do not divulge your password to others because you could be held responsible for their actions (see the Security Policy).

No software other than that approved by the Director Corporate or the Security and Information Management Steering Committee is to be installed on any office equipment. All requests should be submitted to help desk through a division manager.

Members of staff are not to upload any information onto any office IT equipment from a floppy disk, a CD or in any other way if virus controls are not in place.

The use of IT equipment, regardless of ownership, outside the office for the purpose of official business is subject to the following:

• personal computers should not be used at home for business activities if virus controls are not in place
• when travelling, equipment, software, computer drives, files and the like should not be left unattended in public places and portable computers should be carried as hand luggage
• when travelling, portable computers should be provided with an appropriate form of access protection, eg passwords or encryption.

You are responsible for keeping any portable computer in your possession secure. If it is stolen or lost, you must immediately report this to your division manager and the Director Corporate.

You are responsible for keeping any office mobile telephone in your possession secure. If it is stolen or lost, you must immediately report this to the accounts section or the Director Corporate so that arrangements can be made for the telephone service to be suspended.

The division manager is responsible for keeping secure any office mobile telephone that has been allocated to a division for use by division members.

You must take care to maintain the security of information communicated through a mobile telephone or accessed through a portable computer, for example, you should be careful not be overheard when having a work-related mobile telephone conversation with a colleague, and you should make sure that non-staff members cannot read what is on your computer if you are using it outside the office.
9. The office is to be accessible to the public through email

Our internet site and other publications direct people to the general office email address nswombo@ombo.nsw.gov.au. Emails received at this address are cleared regularly. Any email obviously directed to an individual officer is forwarded to that officer electronically with a copy to the division manager or their delegate. Complaints and other general email communications are sent electronically to the nominated team assessment officer.

Staff who have signed and agreed to abide by the office's policy on use of communication devices are able to receive and send external emails from their desktop.

Email may be used where that is the requested form of communication by external parties and/or where the efficiency of enquiries, investigations or other business would be facilitated by the use of email.

Email received at nswombo@ombo.nsw.gov.au will automatically be acknowledged. Emails received from external parties directly to your desktop should be acknowledged in accordance with division protocols.

10. Complaints received by email

It is our policy that complaints received by email are complaints within the meaning of the Ombudsman Act and the Community Services (Complaints, Reviews and Monitoring) Act 1993. The Police Act 1990 specifies that complaints received by email are complaints within the meaning of that Act. Complaints received by email must be handled in the same way as complaints received in other forms, and should be dealt with in accordance with team protocols.

11. Form of email communications

All email communications should conform to the same general standards of language, style and discretion as apply to written correspondence from the office. Emails should always be checked for accuracy, spelling and grammar prior to sending.

12. Authorisation

Any communication sent by email should be in accordance with general office procedures and your level of delegation for the signing of correspondence and any supervision approval requirements applicable. Where approval is necessary, hard copies of the approval should be kept on the file.

Any communication received by email that contains contentious material or involves a complaint about our service should be immediately brought to the attention of your division manager.

13. Clearing email while away from the office

If you are on leave or otherwise away from the office for more than three days, you must arrange to have an automated response to emails installed that advises of your absence and provides guidance on who to call if immediate assistance is required. Alternatively, you can arrange for another officer to have access to your emails, or for your emails to be automatically forwarded to another officer who will undertake to clear them by mutual agreement. Use the out of office assistant function in Outlook to do this. When returning from leave, the temporary email diversion must be disabled.

14. Dealing with CC emails

Copies of complaints sent to other agencies still need to be registered and dealt with according to existing protocols. Generally, non-police complaints of this type will be declined on the grounds of being premature and the concurrent representations.

With other cc emails, especially in cases of complainants who frequently copy to us their email correspondence to others, they should be told that such emails will be noted but will not necessarily be replied to. Action on such emails is at the discretion of the officer responsible for the matter as it would be with copied correspondence sent by ordinary mail.

15. Dealing with complainants who send excessive material electronically

A small number of complainants have been known to take full advantage of the ease of sending material electronically, including sending copies of multiple correspondence to others, photographs, reports, referrals to web sites and other material, much of it not germane to their complaints.
In circumstances where an officer forms the opinion that such communication is unreasonably diverting resources, they should discuss the matter with their supervisor with the view to getting permission to require the complainant to rationalise their communications.

However, such requirements should only be made in exceptional circumstances.

16. Breaches of this policy

Any identified use of equipment or services thought to be inconsistent with this policy or the office’s Code of Conduct will be investigated. Inappropriate use may be subject to disciplinary action and a range of penalties, including termination of employment and/or criminal prosecution.

Members of staff are encouraged to report breaches of this policy to their supervisor or a statutory officer. If an alleged inappropriate use of the internet or email is notified as a protected disclosure, the matter will be dealt with in accordance with the internal reporting policy.

Where inappropriate use is identified the Ombudsman may:

- notify the Independent Commission Against Corruption if there are reasonable grounds for believing the matter concerns corrupt conduct; and
- notify the police if it is reasonably believed a criminal offence has been committed.

OMBUDSMAN APPROVAL

Bruce Barbour
OMBUDSMAN
NSW OMBUDSMAN
USE OF COMMUNICATION AND INFORMATION TECHNOLOGY DEVICES POLICY

UNDERTAKING

I have read and understand the NSW Ombudsman’s policy on Use of Communication and Information Technology Devices and agree to abide by its terms.

I note that the policy constitutes the NSW Ombudsman’s notice of workplace surveillance in accordance with the Workplace Surveillance Act 2005.

I acknowledge that the policy may be amended from time to time. I agree to read any amendment of the policy provided to me from time to time. I also agree to raise with my supervisor any concerns regarding any amendment, including if I do not understand the amendment. I agree to abide by the terms of any amendment.

Name:

Signed: .................................................................................................
PROCEDURES SUPPORTING THE USE OF COMMUNICATION AND INFORMATION TECHNOLOGY DEVICES POLICY

ACCESS TO OFFICE MOBILE TELEPHONES

Mobile telephones are allocated to statutory officers and certain members of staff, as determined from time-to-time by the Ombudsman, who require the use of a mobile telephone to effectively perform their functions.

Mobile telephones are also allocated to each division for use by division members when they are required to work away from the office and need the use of a mobile telephone to effectively perform their functions.

When you take possession of a mobile telephone allocated to your division you must record the following details in the mobile telephone register (to be maintained by the executive assistant or a division assistant):

- the date you took possession of the telephone
- your name
- the mobile telephone number
- your signature.

When you return the telephone, you must place it back in secure storage and record the following details in the register:

- the date you returned the telephone
- your signature.

ACCESS TO OFFICE PORTABLE COMPUTERS

The office’s portable computers are kept in the IT section in a secure cupboard accessible only by the help desk officer.

If you wish to use a portable computer, contact the help desk officer to find out if there is a computer available. Before you take possession of a portable computer, you must record the following details in the portable computer register (to be maintained by the help desk officer):

- the date you took possession of the computer
- your name
- the identifying number of the computer
- your signature.

You must return the portable computer to the help desk officer. DO NOT leave it unattended in their office. You must also record the following details in the register:

- the date you returned the computer
- your signature.

MONITORING AND RELEASE OF BLOCKED EMAILS

1. General

Mail filtering is necessary to protect the office computer network from constant threats in the form of emails. These include viruses which allow people to access our confidential files, viruses which corrupt our data, or spam which can slow down our entire network.
To counteract the thousands of emails sent to staff which may contain viruses or which may be spam, the office uses software to automatically filter all inbound emails. This means an email may be automatically diverted into a safe file accessible only by IT staff before it reaches an inbox.

The rules for determining which emails should be filtered are constantly changing, in order to deal with spam or virus threats which become more sophisticated over time. Therefore, on occasion, more emails may be diverted that usual. IT staff will alert the office when a major new threat has been identified.

Procedures for IT staff to manually release mail are set out in the IT SOPs manual.

2. Mail Marshal

Mail Marshal will be manually checked by IT staff 3 times daily for legitimate blocked mail, as per the Use of Communication and Information Technology Devices Policy. All mail deemed to be unnecessarily blocked will be released.

All Mail Marshal rule sets are documented in the IT SOPS manual. Changes to rule sets require a change approval form.

Users are notified of blocked mail except for messages that are deemed to be spam or to contain a virus. This is consistent with policy and guidelines issued by the NSW Premiers Department.

In practice, users should notify IT helpdesk of a message that they need released, however IT staff may release messages that users have not yet requested for release. Any request is logged in the Help Desk database.

3. Guide for staff about what types of emails will be blocked

All incoming and out going mail is scanned electronically.

Any message that may contain a potential threat to the network, or does not meet policy, is quarantined by the system.

Staff will be notified of quarantined mail, except if the message contains a virus, or is spam.

IT staff will manually review the content of the quarantined messages, and release any messages that do not pose a threat, except if the message contains a virus or is spam.

If a staff member requires an e-mail release urgently, contact IT staff to have it released. If you are missing an email, contact the IT Help desk for further assistance.

THREATS TO THE NETWORK

The following are considered threats to the network, and are blocked. In general these messages are not released:

- virus, worms or trojans - these are quarantined, and not released, and the user is not notified
- spam - any message deemed to be spam is blocked, and the user is not notified
- malformed messages - messages that do not conform to e-mail standards, or are fragmented, are blocked, and the user is not notified.

If you are missing an email, ask IT staff to check that it has not been automatically blocked.

POTENTIAL THREATS TO THE NETWORK

The following messages are blocked, and manually released, after review by IT staff:

- compressed files such as, ZIP, ARJ, RAR
- files with Double extensions, eg: document.doc.jpg, or document.1.doc
- files with attached shortcuts
- files with an unknown file type
- files over 8mb in size
- junk mail, such as chain letters, the Jamie Oliver cookbook, personality test etc. In general, junk mail will not be released.
EMAIL PROTOCOLS

When you use email in your capacity as an employee of the NSW Ombudsman, it is important that you maintain the standards and style of other written communication that you may send on behalf of the office.

Emails sent by staff are subject to the same checking policy/approval process as paper based correspondence, should the content require.

CONTENT

If you are choosing to communicate with an agency or a complainant via email as an alternative to a letter, you should ensure that all of the content that you would generally include in a letter – such as background, summary of inquiries, analysis and recommendations or outcomes – are included in the email. The temptation with email is to tend toward brevity thereby overlooking some of the important information that may need to be communicated regardless of the medium.

STYLE

Sometimes when we use email to communicate the temptation is to be less formal and use language that may be more familiar and abbreviated.

It is important that you use professional language in all email correspondence and avoid any informal discussion that could generate perceptions of bias or conflicts of interests. If the language is overly familiar or personal, were an outsider to examine the correspondence they may infer a personal relationship that could have affected your objectivity and professionalism. This could impact upon the reputation of the office.

APPROPRIATE OPENERS AND CLOSURES

In official communications, take care to avoid using overly familiar greetings to agency contacts or complainants, such as ‘hi’, asking personal questions, such as ‘how was your weekend?’ before turning to the business at hand, or signing off with ‘warm regards’, ‘cheers’ or similar. Such terms can create a perception of bias, even if unfounded. While email can be a less formal means of communication, it is important that all our email communication is seen to be impartial by recipients and third parties alike.

Appropriate openers:

- [First name]
- Dear [first name]
- Dear [title] [last name]
- Hello [first name]
- Hello [title] [last name]
- [Nothing]

Appropriate closures:

- Thank you/Thanks [followed by your first and/or last name]
- Regards [followed by your first and/or last name]
- Yours [followed by both your first and last name]
- Yours sincerely [followed by both your first and last name]
- Yours faithfully [followed by both your first and last name]
- [Nothing other than your first and/or last name]
SUBJECT LINE IN EMAILS

The subject line, when pursuing a complaint with an agency, should consist of:

‘Your ref: xyz; Our ref: ****’.

The name of the complainant/case should be in the body of the email in the first line as:

Re: Joe Bloggs Complaints

Leaving the name out of the subject line increases security. If the agency’s reference includes the name then that should appear at the start of the body of the email.

WHAT TO DO WITH PERSONAL CONTENT IN OFFICIAL EMAILS

There will be times when we know agency contacts well enough to exchange personal comments such as ‘what are your plans for the weekend?’ or ‘how did the race go last week?’. These comments should be put in a separate email or better still, make a telephone call. If you receive an email combining personal and official matters you should ask the contact to resend the official email without the personal matters, so that you can put the response on file.

RECORDKEEPING

All work-related emails must be logged in TRIM. You will need to rename emails when saving them into TRIM to better describe their content so they can be searched.

Often messages become a series of replies. For the purpose of good recordkeeping, in the case it makes sense to capture the last message in the series, which will include all previous exchanges, rather than separately capturing all of the messages.

EMAIL SIGNATURE

In order to ensure all emails coming from the office have the same sign-off, we have developed a standard email “signature” for staff. Information about how to set up and set an electronic signature can be found in ADM/65.