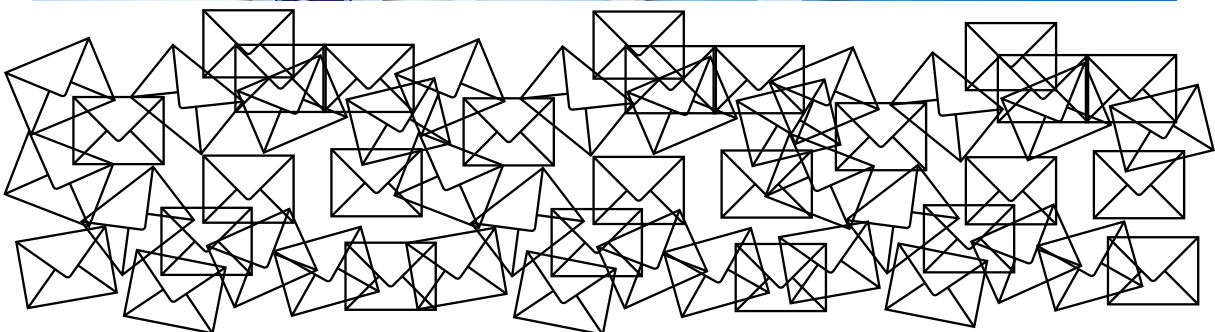
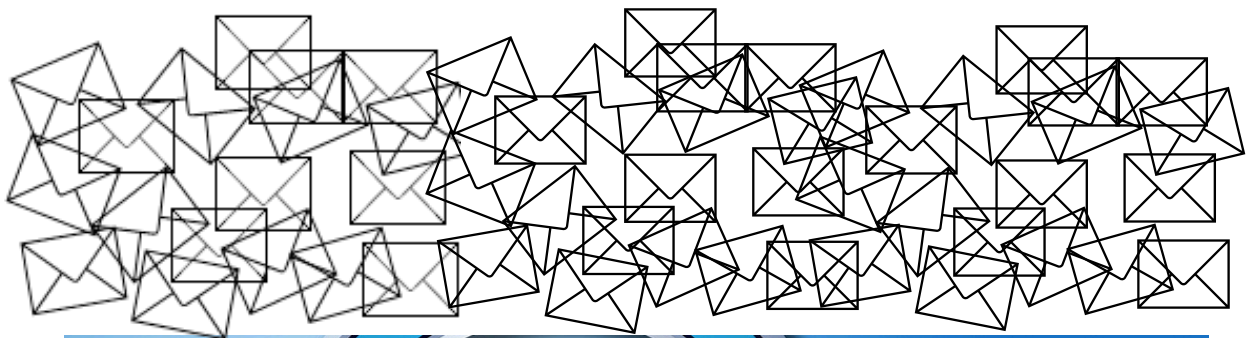




EMAIL MANAGEMENT

Governance Services



Jase Digital Media

Do you send and receive emails as part of your job? Yes? You are therefore **responsible** for ensuring that all emails you deal with in the course of your employment with the University are managed in line with the University’s Email Policy, Information Security Policy, Records Management Policy and others as detailed on page 20.

Contents

Introduction	4
Legislation	4
Security	7
Access.....	7
Routine Management	7
Retention Periods	8
IDENTIFYING AND MANAGING EMAILS WHICH ARE RECORDS	9
1. Identifying Email Records.....	9
2. Responsibility for Keeping Email Records.....	10
3. Where to File Email Records	11
4. Titling Email Messages in Electronic Record Keeping Systems.....	12
Email DOs and DON'Ts	14
GENERAL GUIDANCE FOR USING EMAIL.....	15
1. When to use Email	15
2. Creating and replying to messages	15
2.1 Subject.....	15
2.2 Addressing messages	16
2.3 Content and tone	16
2.4 Structure and grammar.....	17
2.5 Advice from the Marketing and Communications Department	17
3. Email attachments	19
4. Managing email communications.....	19
5. Managing your inbox	20
6. Email when out of office	21
6.1 Guidance for Managers.....	21
7. Email accounts of leavers.....	22
8. Use of generic email addresses.....	22

<p>'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive. (NOT the H: Drive, C: Drive or MySite – these are not shared)</p>

9. Personal Use	23
10. Allied Internal Policies.....	23
11. Further information	23
11.1 Information Security Policy: Email and Internet Use.....	23
11.2 Electronic Information Security Policy: Monitoring and Logging	24
11.3 Email Security Guidance.....	25
11.4 Data Protection Code of Practice: Email and Personal Data	26
11.5 Email encryption information and guidance.....	27
11.6 General Outlook email information and guidance	28
Email FAQs	29
Why do I need to save email records on a shared drive?.....	29
How long do I keep emails?	29
1) Records	29
2) Copies of emails sent to others/attachments	29
3) Reference material	29
4) Ephemeral/Transitory Records.....	30
5) Emails retained for your personal	30
Can emails form a contractual undertaking?.....	30
Is any email/Outlook guidance available?	30
Strategies to avoid email overload	31
Index.....	34
APPENDIX A – Quick Reference Guide.....	35
APPENDIX B – Simple Steps to Effective Business Emails	35

<p>'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive. (NOT the H: Drive, C: Drive or MySite – these are not shared)</p>
--

Introduction

“For any organisation, a failure to manage emails indicates a failing in records management generally” The National Archives, 2010

Email is one of our preferred methods of conducting University business, however as more business is conducted this way keeping on top of managing your emails becomes more difficult. Although, ideally we would all like to have clear inboxes at the end of each day the reality is that this seldom happens, *however it is the individual **responsibility** of every University employee to ensure that they manage their time to accommodate the management (sorting, filing and disposal) of emails as failure to do this puts the University at risk in a number of ways.* The predominance of business being conducted by email also means that the likelihood of emails being official ‘records’ is greater than ever before.

A few important points to remember are:

- The University email system is a **communication tool NOT a filing system**
- Personal data disclosures by email are the second most likely way in which **data breaches** occur according to the Information Commissioner’s Office.
- Nearly 40 FOISA appeals dealt with recently by the Scottish Information Commissioner involving Universities required information which was included in emails.
- Emails documenting decisions and evidence of business transactions are **RECORDS** and therefore subject to the same **legislation** and other requirements as records held in other formats.
- Records kept in individual University email accounts are essentially being filed in a **personal storage area** and are therefore **not accessible** to others who may need to see them.
- Emails should be **routinely managed** and stored along with other records pertaining to the same task/subject/business.

Expanding on these points briefly...

Legislation – there are time limits (**retention periods**) enacted in law which stipulate how long we should keep certain information. Keeping information for too long or deleting it too early leaves the University (and you personally) at **risk** of breaking the law or possibly facing disciplinary action.

Legislation – The applicable legislation is listed below along with a brief outline of the main relevant notes which include best practice guidelines where necessary:

‘Shared network area’ refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

Computer Misuse Act 1990

This Act makes it an offence to:

- Maliciously corrupt or erase data or programs e.g. download from a received email or send an email containing viruses or malicious software, thereby denying access to authorised users or giving unauthorised access;
- Make unauthorised use of computer facilities or unreasonably waste computer resources and time.

Data Protection Act 1998 and General Data Protection Regulation 2016

- This Act protects the rights and privacy of individuals' personal data e.g. contained in text, images, audio recordings, etc. Email users must be aware of the risks associated with sending personal data externally by email and ensure these are carefully considered in order to avoid a data breach e.g. must consider if encryption or password protection the information is required. Guidance can be found in the University's [DP Code of Practice](#), [encryption advice](#) and [email guidance](#) and [Information Security Classification Scheme](#)
- Individuals are entitled to request a copy of any information held about them e.g. their personal data - this includes information in email format. It is an offence to alter or destroy that information once the data subject has submitted a Subject Access Request. Care should be taken not to include inappropriate comments in emails which may be disclosed in response to an access request.
- Under this, and related, legislation [University policy](#) is that members of staff should not grant another individual access to their email account unless exceptional circumstances apply and it is authorised by a senior manager.

Privacy and Electronic Communications Regulations 2003 (PECR) (and e-Privacy Regulation due in 2018)

These regulations protect individuals' privacy, with particular regard to regulating electronic direct marketing activities.

- Consent by affirmative action must be collected from individuals before they can be sent any communications designed to influence or change recipients' behaviour. Consent must be as easy to withdraw as to give and records of consent must be maintained. Opt-out tick boxes are *not* allowed.
- Any approved email marketing activities must adhere to the [University PECR guidance](#).
- Sending unauthorised, unsolicited marketing material, chain letters and 'junk' mail of any kind from University email accounts is prohibited.

Freedom of Information (Scotland) Act 2002 (FOISA)

- This Act gives individuals the right to request information held by public authorities, including information contained in emails.
- Email records must be retained in shared network areas, which comply with University guidance, having the appropriate level of security required for the type of information and being accessible to appropriate colleagues, to ensure that the information is available for FOISA responses and any other business reasons.

- Under section 61 of the FOISA the University is obliged to observe the Scottish Ministers' Code of Practice on Records Management, which includes the management of emails which constitute University records. The University's [Records Management Policy](#) and [email guidance](#) refers.
- Protected and/or Confidential information must be handled in accordance with the recommended Security Controls detailed in the [University Information Security Classification Scheme](#). Information in these categories must not be transmitted/shared for unauthorised purposes.
- University business should not be conducted by employees through non-University email accounts – any such communications are subject to FOISA.

Regulation of Investigatory Powers Act (Scotland) 2000

- This Act regulates the surveillance and investigation of communications by institutions and makes it an offence for any person to intentionally and unlawfully intercept communications.
- The University conducts authorised monitoring as detailed in the [University Monitoring and Logging Policy](#) (Electronic Information Security Policy) and the [University's Personal Data Processing Statements](#).

Copyright, Designs and Patents Act 1988

- Intellectual property legislation makes it an offence to use or copy all or a substantial part of any work/s, registered or unregistered, which are protected under the legislation, without permission or acknowledgement, including sending or forwarding the work/s by email.
- Confidential information such as business plans and trade secrets are covered by the Act. The University has a [comprehensive copyright guidance resource available online](#).
- Other legislation dealing with intellectual property rights includes:
 - [Trade Marks Act 1994](#)
 - [Intellectual Property Act 2014](#)
 - [Communications Act 2003](#)
- It is an offence to send a message or other content that is grossly offensive or of an indecent, obscene or menacing nature or where the sender's address is masked or 'anonymous'. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false. An offence is committed as soon as the message has been sent: there is no need to prove any intent or purpose.
- Other legislation which deals with written communications which are threatening, abusive, defamatory, discriminatory, inflammatory or insulting and cause alarm, distress or any form of harassment are:
 - [Criminal Justice & Public Order Act 1994](#)
 - [Equality Act 2010](#)
 - [Protection from Harassment Act 1997](#)
 - [Sexual Offences \(Scotland\) Act 2009](#) (section 7 refers)

<p>'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive. (NOT the H: Drive, C: Drive or MySite – these are not shared)</p>

- o [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)

Please note that this list is not exhaustive.

Security - email is NOT a secure medium! Consider how easy it is to send an email to the wrong recipient, and what if that email contains personal or sensitive information? Outlook helpfully assists in this regard with the 'Auto-Complete' address functionality. Additionally, sending unencrypted emails containing personal or sensitive information which can be intercepted is a **high risk** practice, as is sending long email conversations, where there is a greater **risk** of confidential information being 'buried' in the trail. Bear in mind that emails are also stored on various servers belonging to various internet service providers en route to their destination/s.

Security - many employees nowadays access their University email accounts using mobile devices – if you are accessing your email on your mobile/smart phone and don't have the necessary security precautions in place (passwords, Airwatch app, etc. as per [IS guidance](#)) your email account is potentially vulnerable to thieves and anyone else who may have access to your phone. If you are keeping sensitive or personal information in your email account for 'safety' and accessing it this way you are at **risk** of breaching both legislation and University policy.

Access – keeping information and records in your University email account means that they are effectively being kept in a personal storage area. Records which are evidence of decisions or University business must be kept in a shared network area like SharePoint or the S: Drive where at least one other person has access. There have been occasions where someone has left the University and important records which were kept in their University email account have been lost. If the information is someone's personal data, sensitive or confidential information it must be kept in an appropriately secured folder in the department's SharePoint site/S: Drive with access given to the necessary staff members. Not ensuring that the appropriate colleagues have access to information is **risky** for the University.

Routine Management – make efficient use of time by dealing with an email the first time you open it, then classifying it and filing it. Initial classification may be by deciding if the email is:

- a) A record of University business
- b) For reference only
- c) Personal
- d) Spam/Junk mail

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

Once this has been done the email can be further categorised and saved on SharePoint/S:Drive with related records if necessary. In the case of emails which constitute records of University business it is **imperative** that this is done to ensure that:

- i) the correct retention period is applied in accordance with your department's Records Retention Schedule and the email is kept for as long as is necessary and no longer
- ii) the record is available to more than one person. If the record contains personal, sensitive or confidential information the access permissions on the site/folder in which it is kept on SharePoint/S:Drive must be restricted so that only people with the necessary permission have access...even if this is only yourself and your manager.

Further categorisation of records will be by the type of record and by the business activity/process to which they relate. Site/folders should already be set up on your departmental SharePoint site/S: Drive to receive these records and keep them with other related records. You need to consider the following when categorising email records:

1) **Records containing personal, sensitive or confidential information** – save on SharePoint/S:Drive with related records to ensure that the records are retained/destroyed in accordance with your department's Records Retention Schedule. Restrict access permissions as necessary.

2) **Records of routine business information/correspondence/transactions** - save SharePoint/S:Drive with other related records to ensure that records are retained as long as necessary and destroyed in accordance with your department's Records Retention Schedule.

3) **Transitory/temporary/ephemeral records** - some of these, such as office information, announcements, cc'd messages for information only, meeting reminders, telephone messages, etc. may be deleted immediately or shortly after receipt, when the contents are no longer relevant. Others, which are of use in the short-term and contribute to the compilation of minor records can be saved on SharePoint/S:Drive with the relevant retention periods/deletion dates applied to them. Further guidance for these types of records can be found on the [Governance Services/Records Management pages on the staff intranet](#).

Please see below for further guidance on emails which are **records of University business**.

Retention Periods

Generally speaking, the length of time which emails should be kept is as follows:

a) **Records** – in accordance with departmental Records Retention Schedules

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

b) Reference Material – delete once read or used. Retain on SharePoint/S:Drive in the interim if necessary along with the information and/or records to which the reference material relates in a folder called ‘Reference Materials’ then further subcategorised by month/year to assist with deletion, or alternately in a filing structure which informs the use of the information and when the information should be deleted e.g. by subject then month/year

c) Personal Correspondence – delete once used. Retain on H: Drive if the correspondence relates to your employment – set review/deletion dates

d) Spam, junk, unsolicited or suspicious messages – delete.

IDENTIFYING AND MANAGING EMAILS WHICH ARE RECORDS

Email messages often constitute important records of University business and need to be managed in the same way as other University records to ensure that information can be located when needed and is disposed of according to the appropriate records retention schedules which document University policy on retention and disposal. The following provides guidance on measures that can be taken to effectively identify, retain and manage the emails created and received by the University which constitute our business records.

Please note that the following guidance applies to generic departmental email accounts which can be accessed by multiple members of the team, as well as email accounts allocated to individuals. Generic departmental email accounts must be assigned an active supervisor whose responsibility it is to ensure the email account is managed in accordance with this guidance.

1. Identifying Email Records

A record has been defined as “*information created, received and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business*” [BS ISO 15489: 2001).

In broad terms, an email will be considered a record where it provides evidence of University business related activities, events and transactions which have ongoing business, compliance, operational or historical value.

The following (non-exhaustive) list of criteria should be considered when determining whether or not an email needs to be retained as a record.

If the answer is **YES** to any of the questions below, then the email is a record:

Does the message:

- Contain information which may need to be provided as evidence in a court of law if the University’s decision is challenged?
- Contain information which documents University decisions, including the discussion showing how the decision was arrived at?

‘Shared network area’ refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

- Document the formulation and execution of policy?
- Contain information upon which University business decisions will, or are likely to be, based?
- Commit the University or its staff to certain courses of action including the commitment of resources and provision or purchase of goods or services?
- Document the establishment, negotiation and maintenance of business relationships with clients (including staff and students)? For example: provision of information or a request from a student.
- Record contractual undertakings entered into by the University?
- Have long term value for future reference or historical purposes?

Is it needed to:

- Prove a business related event or activity did or did not occur?
- Demonstrate the initiation, authorisation or completion of a business transaction?
- Identify who took part in a business activity?
- Satisfy legal/compliance purposes?
- Facilitate business analysis and reporting?
- Display public accountability for policies or decisions?

If none of the criteria above are met, it is unlikely that the email has any record value. Specifically, emails should **not** be considered as records where they are:

- Circulated for information or reference purposes only e.g. event announcements
- Of short term operational value e.g. meeting arrangements
- Mass circulated communications received from external agencies which require no action and are not required for 'record' purposes. These may include newsletters, magazines, product information and flyers
- Personal.

Non-record emails can be deleted as soon as they are no longer needed. This should be done as soon as possible.

2. Responsibility for Keeping Email Records

When determining who has responsibility for capturing and keeping the "official" copy of an email record, the following conventions should be observed. **Please note:** This is a general rule to which there may be exceptions.

For internal (e.g. staff to staff) email records sent or received:

- The sender or initiator of the dialogue forming a message string is responsible for keeping/filing it, as there is one sender and possibly multiple recipients.
- If action is required by recipients, or the recipient is responsible for keeping the record on the matter communicated, they should also keep a copy

For email records sent externally (including from staff to student):

- The sender is responsible for keeping

For external email records received (including from students):

- By one person – the recipient is responsible for saving the email with related records in SharePoint/S: Drive
- By multiple recipients – the person responsible for the area of work relating to the message is responsible for keeping e.g. an email from Universities Scotland containing information about a Freedom of Information issue received by the Principal, Director of Information Services and Governance Services. As Governance Services is responsible for Fol compliance, they keep the record copy.

When saving email **attachments** consider if the email needs to be kept with the attachment to give it context e.g. proof of who send it when. Generally, for attachments received from an external source the email and attachment should be kept together. This may also be the case for attachments received internally, but further guidance is given in [Section 3](#) e.g. send links not attachments if possible.

All other duplicate copies of record email messages can be deleted by users when no longer needed.

When saving email **conversations (long strings)** it is sufficient to keep the last message (which contains the entire conversation) and delete the others (partial sections of the conversation), as long as their content is included in the 'string' being saved and have not been altered in any way. If the conversation has been copied to others, who have contributed separately, it may be necessary to save the various strings to ensure that an entire record is preserved.

See [section 4](#) for guidance on email communications which may become long conversations or strings.

3. Where to File Email Records

Email messages which are records should be moved out of the email system into a shared network area like SharePoint or the S: Drive where they are kept in one place with all related records and accessible to all staff working in the same business area as appropriate. This can be done by saving the email/s to folders within the departmental Sharepoint site/S: Drive, but can also be achieved (less desirably) by printing to paper and filing in paper based filing systems.

The periods for which records need to be retained are determined according to business and regulatory requirements. Guidance on the retention of University records is available on the [Governance Services](#) intranet site.

Departments should have filing structures in place which relate to the activities they undertake in the course of business. Ideally these filing structures should be

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

arranged according to the Functions, followed by the Activities or business processes and lastly the tasks undertaken to complete the business processes. If you have any queries about how these should be set up or need guidance on how to improve your filing structures please contact the Governance Adviser (Records Management) on extension 6359.

Emails must be moved out of the email system and into an [approved filing structure](#) (SharePoint recommended) as soon as possible. They must retain their original context, content and structure and adequate metadata to ensure that they are legally admissible and can be used as evidence in court in the event of a dispute.

Once saved to Sharepoint/S: Drive you should delete the original message from the Outlook mailbox.

If you are saving an encrypted email ensure it has been unencrypted before it is saved to the shared network area/folder.

4. Titling Email Messages in Electronic Record Keeping Systems

When an email message is saved into an electronic folder on Sharepoint/S: Drive, the title ('subject') of the resulting .msg format file, which defaults to that of the original email message, is the main way in which the email record will be identified and retrieved. However, in many cases the title of the original message will not reflect its content or the reason for capturing it as a record and will make subsequent identification and retrieval difficult.

The naming conventions applied to related records in other formats e.g. Word or Excel are equally applicable to emails. The department should have set naming conventions for all records relating to each business process, as those used for meetings will not follow the same format as those used for policy development or student records.

To facilitate the easy identification and retrieval of saved email records, the following conventions should be observed:

- If the default title of the saved email does not accurately reflect the content of the message then the .msg file title should be changed. For example, titles such as *"RE: Fol Request"* provide no information on content or purpose that would help identify relevant records relating to a particular case.
- The file title should provide sufficient information to identify its content.
- The file title should use natural language and spell words in full.
- The prefixes *'RE'* and *'FW'* should be omitted from titles as they provide no information on the message content.

For example, a series of emails saved to an electronic folder with the default titles *"Fol Request"*, *"FW: Fol Request"* and *"RE: Fol Request"* can be more meaningfully renamed as follows (each FOI request is assigned a unique number for ease of reference).

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

FOI Request 14-123-Expenses-Request
FOI Request 14-123-Expenses-Finance Consultation
FOI Request 14-123-Expenses-Response

N.B It is only the .msg file that should be renamed. The title of the original message within the file must not be altered.

Further guidance is given below on constructing informative and useful titles in the email 'subject' field and generally on naming conventions on the intranet [Records Management pages](#).

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

Email DOs and DON'Ts

✓ DO	✗ DON'T
Remember that emails sent and received on University systems are subject to multiple pieces of legislation and policies and may be open to scrutiny or required for legislative purposes. Please see guidance at end of document.	Send business emails to or from staff member private/non business email accounts.
Remember that University systems are for University business , and save emails which are University records into Share-Point/S:Drive with related records, ensuring appropriate access controls are in place.	View emails to do with University business as your personal correspondence.
Remember that the University email system is not a filing system /information storage repository.	Leave all your messages in the University email system e.g. Outlook or a .pst archive
Remember that email is NOT a secure form of communication. Encrypt emails containing personal, sensitive or confidential information.	Send any personal, sensitive, or confidential information as a general rule.
Filter the emails you receive and decide if you should Act, Read or Delete them.	Keep important University records in your email account – particularly if they are the only copy (Golden copy). They may be needed by others in your absence.
Delete non-record emails as soon as they are no longer useful or required.	Forget to empty the 'deleted' folder in your email account regularly.
Provide links to files in the message body rather than sending attachments.	Send attachments – send links where possible.
Set time aside regularly to manage (review, file or delete) emails in your account. Set up an appointment in your calendar for regular review.	Allow backlogs of emails to accumulate in your account. This can lead to their management becoming an 'insurmountable obstacle'. Mass deletion of emails increases the risk of destroying records too early in contravention of legislation/policy.
Use one email per business item , so that they can be stored with the other related information/records.	Mix University and personal business in one email.
Use appropriate business language , as you would for any other business records/communications. Remember that emails are subject to information legislation.	Send angry emails or make inappropriate comments which would cause embarrassment if the email was required to be produced in response to a Subject Access or FOI request.
Be Efficient: deal with the whole process for an email in one pass as often as possible – read/action then file/delete as appropriate.	Waste time by leaving emails in your inbox that you will return to or re-read just to make sure they have been dealt with.
Title your email in the 'subject' field with useful, precise information .	Send long convoluted messages that are hard to understand.
Use the 'CC' facility with care	Use BCC, rather forward the message.

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
 (NOT the H: Drive, C: Drive or MySite – these are not shared)

GENERAL GUIDANCE FOR USING EMAIL

1. When to use Email

We should all consider the whether or not email is the most appropriate or timely method of communication for the situation. Depending on the subject matter, telephone calls, short memos or meetings may be a better alternative. For example:

- Complex, technical or potentially confusing subject matters may be best communicated either by phone or a face to face meeting
- If the matter requires a quick response, use the phone, backed up with a file note where appropriate

Managers should avoid unnecessary use of email discussion of employee performance issues. This minimises the risks of messages being mis-sent or comments misinterpreted and it could create unnecessary records which are subsequently required to be released via Subject Access Requests (see [Data Protection Code of Practice](#)). Copying in others to these emails can then create a web of correspondence which is difficult to follow and creates multiple copies of conversation threads which are both difficult and time consuming to prepare for disclosure. **A good tip** here is that if a matter does not require a record to be kept, find an alternative method of communication.

2. Creating and replying to messages

The following guidance is based on best practice and can also be applied easily to other written records.

2.1 Subject

The subject line or title is one of the most important parts of the email – compose it for maximum impact and usefulness. A well chosen heading will identify the business being dealt with, giving enough detail for the recipient to determine the contents and enabling them to prioritise the message and deal with it efficiently (including filing/saving email records in a shared network area). Poorly chosen email subject lines are inconsiderate to the sender as they require extra work to process and manage e.g. reading the whole email before realising at the end what it is about and having to waste time by coming back to it later because of time constraints.

Under no circumstances should the subject line contain individuals' names or include other sensitive personal information in the subject of the message e.g. "*Disciplinary Procedure: Joe Bloggs, Matriculation Number: 1234567*".

- Limit email to one subject per message, this makes it easier to deal with and is likely to lead to a quicker response.

- When creating the subject matter, be as precise as possible. Instead of simply using “Meeting minutes” which is too vague, consider “[*Meeting name*][*date*] minutes to discuss [*subject matter*]”. Take into consideration any naming conventions which may be used to file the message in a shared network area – doing this correctly the first time reduces work in updating/changing the subject line when saving email records in a shared network area later.
- Prefixes - indicate in the subject matter box what action is required, if any, from the reader e.g. “for action” or “for information only” (which indicates that no reply is necessary). Avoid using acronyms which may make your email look like spam. Avoid using ‘urgent’ as a subject line prefix – if your communication is urgent it is preferable to phone the intended recipient.
- Use Outlook flags to indicate whether the message is of “high” or “low” importance. If an *internal* email contains personal or confidential information please use the ‘message options’ to indicate to the recipient that the content is of a sensitive nature. Emails being sent to *external* parties which contain personal or sensitive/confidential information **must be encrypted**.
- [Information Security Classification scheme](#)

2.2 Addressing messages

When deciding who to send messages to, colleagues should consider the following:

- Only send messages to staff who actually need to know
- Only include recipients in the “To” field who are expected to act or take decisions based on the message content
- Include recipients in the “CC” field for information only and consider whether they really need to know. Including a senior member of staff may mean that they HAVE to take action – it may be more appropriate to give them an update separately.
- Avoid the use of the “Bcc” function as messages should have a clear, auditable trail. **IF** the message is to be passed on someone else, use the “Forward” function instead
- Use the “reply all” function with extreme care. It is unlikely that everyone included in the original message will need to know your reply.

2.3 Content and tone

When composing the message, you should:

- Make the main point early on in the email
- Keep your email brief and to the point, avoid lengthy rambling emails.
- Use neutral, professional language and tone – assume that anything you write will be published. Emails can provide contractually binding agreements and are often official University records, therefore exercise the same degree of care and professionalism in regard to the content as you would to any other communication.
- Do not use ill-advised comments on individuals and ensure that you differentiate between fact and opinion – you may delete your copy, but others will be stored on servers and possibly by recipients and may be forwarded to others. Remember that even though you may delete your copy of an email, the recipient and potentially others might retain theirs.

- Avoid angry emails – monitor the tone of the message and do not reply immediately; take some “time-out” before responding and then re-read your reply before sending
- Take care to ensure that the message is inoffensive and cannot be construed as harassment, discriminatory, abusive and offensive. Messages must comply with [Edinburgh Napier’s Information Security Policy](#).
- Take into consideration that email as a business communication is often not as formal as a letter and open to misinterpretation.

2.4 Structure and grammar

The overriding assumption is that emails are subject to external scrutiny and so care should also be taken over the structure, grammar and punctuation when writing an email message. Ideally, you should:

- Use plain English as far as possible and avoid abbreviations.
- Use paragraphs to structure information.
- Position important information at the beginning of the message.
- Proof-read your email before sending.

Business email communications with “text-speak”/abbreviations, spelling and grammar mistakes look unprofessional. Consideration should be given as to how you would compose your message if it were a formal letter or inter-office memorandum (memo) – which is what email essentially are...they replace telephone calls, paper letters and memos. Consider using a memo template in Outlook.

2.5 Advice from the Marketing and Communications Department

Email etiquette

Sending an email is the equivalent of using Edinburgh Napier University letterhead paper. Be courteous, check spelling and grammar and read back over messages before sending.

- Always fill the ‘Subject’ field with a short, but meaningful, description.
- NEVER USE BLOCK CAPITALS – it’s the equivalent of shouting.
- Resist the temptation to use backgrounds or colours; these can make the email difficult to read.
- Black 12pt Arial or Titillium should be used whenever possible.

Email signatures

To ensure consistency across the University, all staff are requested to update their signature to the following standard layout utilising Arial or Titillium 12 point font.

Example signature:

Professor Peter Starling PhD
Head of Research
School of Computing
Edinburgh Napier University
Merchiston Campus
Colinton Road
Edinburgh EH10 5DT
T 0131 455 6789
M 0771 234 5678
E p.starling@napier.ac.uk
W www.napier.ac.uk

If you work internationally, you may want to add Scotland to your address and add the prefix +44 (0) to your phone number, eg +44 (0)131 455 6789

Message about the University

If you wish to include a message beneath your signature promoting the University please use the following message:

At Edinburgh Napier we nurture talent and create knowledge that shapes communities all around the world.

Our innovative research provides solutions to society's challenges, our graduates leave ready for the workplace, and we have wide-ranging links with employers and business.

If you wish to promote a specific departmental initiative or your programme please be careful to keep this message up to date and accurate. Graduate employability statistics and league table rankings change every year, so you should ensure that you are using the most up to date version. If in doubt please contact the Marketing and Communications department via marketing@napier.ac.uk who can provide you with the most up to date messaging.

3. Email attachments

Email attachments take up the bulk of storage space on the email system and should be avoided wherever possible – they contribute to the proliferation of copies on the system and make version control difficult.

Wherever possible a hyperlink to the file should be included in the body of the email message – **avoid sending attachments** if the recipient has access to the file on SharePoint or another shared network area. If there will be ongoing work or collaboration consider setting up a SharePoint site for this purpose. Sending attachments increases the chances of multiple copies of the same document/record being stored across the University's network and of multiple versions being created and worked on. The proliferation of copies of email attachments not only takes up valuable server storage space, but also slows down the email system (Outlook).

Emails with attachments which are University records must be saved and filed in their entirety (including links, graphics, etc.), in order for them to maintain their content, context and structure and therefore be full and accurate records – having the attachment without knowing where it came from or when means that it has lost some of its context and is incomplete (you might know now, but saving them together preserves the information for others over time).

If the attachment requires further work, file both the original message and attachment together and save a separate copy of the attachment to work on. This separated attachment then becomes a new and distinct record and version control must be applied.

4. Managing email communications

When managing email conversations with one or more people, the following should be observed:

- Restrict the message to one topic and try not to stray from it. Messages containing more than one topic are difficult to file and manage.
- If the subject changes significantly within a message string, you should begin a new string and change the title when you respond.
- Always reply with the original text thereby ensuring a management trail. This provides context to your response and allows a complete record of the exchange. Longer conversations can be cut off so that your response contains only relevant information, preferably only the last message to which you are responding.
- If a conversation needs to include others part way through start a new message with the relevant information or arrange a meeting (see next point)
- If the string is becoming or is likely to become unmanageably long consider arranging a meeting with the recipients/contributors to discuss the issue/subject. Try NOT to let message strings develop beyond ten (10) messages as this increases the risk of:

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

- The message not being read/information being missed by the recipient/s
- Personal/confidential/sensitive information being sent/received in error
- Do not annotate the original text in your response. Any formatting to distinguish your comments from the original text can easily be lost if any alteration is made to the original message format.

5 Managing your inbox

University employees are provided with 50GB of storage space in the individual email account they are allocated, however you should keep storage to a minimum to avoid performance and technical issues such as slow system response times and the risk of file corruption or loss. You are required to actively manage your email account to keep storage requirements to a minimum.

Useful tips which may help you manage your mailbox:

- Allocate a fixed period of time in your schedule to read through and sort messages – even if it's only a short period of time; don't leave it until your emails are unmanageable.
- Consider the sender, subject line and any flags to gauge the importance of a message.
- Prioritise which messages need to be dealt with first.
- Use Outlook functionality to set up a flag to indicate where you have been cc'd into email messages. Often these will be for information and will not require immediate, if any, action on your part.
- Use folders to group related messages together.
- Identify record emails and move them out of the email system promptly.
- Promptly delete low value, non-record messages which are no longer needed.
- Use Outlook functionality where appropriate to set up rules, such as automatically moving messages sent to particular addresses to folders or flagging messages received from particular addresses. However, ensure that you check these folders. If there is a possibility that you might not see something important because you have applied rules it would be best not to apply rules and let the email come into your inbox for checking. If you have signed up to an email alert service or distribution list service/forum and are not reading the emails routinely consider 'unsubscribing' from the service or see if you can refine.

6. Email when out of office

If you are going to be out of the office, you should always set an 'out of office' or automated reply message indicating when you will return and providing an alternative point of contact and if possible a generic/departmental email address which colleagues will be monitoring. This is essential if we are to conduct our business effectively, and ensure we deliver our statutory commitments.

It is also useful to remember that we are **all** bound by the Freedom of Information Act and the 20 working day timescale – if you receive an FOI request and are away from the office the statutory deadline for the University to respond will start from the day the email is received and the Information Commissioner will not take any individual's absence from work into account if the deadline is not met and a complaint is subsequently received by the Commissioner. To ensure that applicants can redirect their requests for information **all University employees** should include the following text in their 'Out of Office' automated replies:

If your email contains a request for information that you feel may fall under the Freedom of Information (Scotland) Act, please visit our [FOI website](#) . Alternatively, visit www.napier.ac.uk to check for the information you require. For routine enquiries see <http://www.napier.ac.uk/about-us/contact-us> and for feedback on the website [click here](#)."

Do **NOT** grant a colleague(s) proxy access to your inbox or auto-forward/ automatically re-direct emails to colleagues – there are various legislative implications to take into consideration and the expectations of the recipient as to who will be reading/receiving the communication. Do NOT give out your computer log-in ID to anyone to check your emails either, please refer to the Information Security Policy (link provided below).

6.1 Guidance for Managers

Staff members who are unexpectedly out of the office

The line manager should contact Information Services and request that they set up an 'Out of office' message for the member of staff saying:

'I am currently out of the office with no access to emails. Please re-direct your email to <colleagues name and contact email OR departmental generic email account address>.

If your email contains a request for information that you feel may fall under the Freedom of Information (Scotland) Act, please visit our [FOI website](#) . Alternatively, visit www.napier.ac.uk to check for the information you require. For routine enquiries see <http://www.napier.ac.uk/about-us/contact-us> and for feedback on the website [click here](#)."

The message should be generic and not provide any information alluding to the reason/s for absence or personal information.

7. Email accounts of leavers

Before leaving Edinburgh Napier University, you should:

- Ensure that you have moved all email records out of any email account folders that you use to conduct University business and to which you have sole access and into the established filing system (electronic or otherwise)
- Delete all personal and non-record emails from your account
- Set an “out of office” message giving an alternative contact

Managers should:

- Confirm an out of office message has been set on the last day
- Ensure that the leaver gives permission for their Outlook account to be accessed for University information and records.
- Arrange with Information Services (IS) for access to the account if records of University business/records/messages are still held on it

If you are changing roles within the University, especially if you are moving to a new department/team, you should also observe the guidance above relating to email records. Managers should ensure that any emails relating to their department/team are saved in the established filing system in a shared network area for colleagues to access as necessary.

8. Use of generic email addresses

Where possible, generic email addresses, accessible to a group of people, should be used in preference to individual email addresses. A generic email address is one that reflects a business grouping, function or role e.g. health&safetyoffice@napier.ac.uk, or ugadmissions@napier.ac.uk. A generic email account must be assigned an active owner or supervisor who ensures that email messages are not left to accumulate in the account, but are managed appropriately and stored in SharePoint/S: Drive.

This allows a consistent contact point which will not change when staff change role or leave. It also helps minimise the risk of having to amend mailing lists, web references and printed materials thereby ensuring a degree of longevity. It also ensures a group of staff can access the generic mailbox to retrieve and action messages, reducing the risk of messages lying unattended in the individual mailboxes of absent staff

Organisational measures should be in place to ensure that generic mailboxes are regularly checked and appropriately managed. The same guidance as given above applies – emails must be filtered and saved in a shared network area (e.g. SharePoint or the S: Drive) or deleted as appropriate, and should NOT be left unmanaged with a build-up of email messages. Remember that Outlook is NOT designed to be a filing system or storage area for messages – keeping too much information in Outlook can cause technical errors or failures in the system and makes retrieval of information time consuming and inefficient.

9. Personal Use

As detailed in the Information Security User Policy (section 6), the University permits personal use of systems subject to a number of conditions as long as this does not interfere with, or impinge on, University business in any way. It is not recommended that the individual email account allocated to users by the University is used for personal communications, especially not routine personal business or communications. Users should be aware that the University reserves the right to monitor the use of all the systems it provides, including email (please read the [Information Security Monitoring and Logging Policy](#)). Keep personal emails to a minimum to avoid using University server storage space

10. Allied Internal Policies

- [Data Protection Policy Statement](#) (and [Code of Practice](#))
- [Electronic Information Security Policy: Monitoring and Logging](#)
- [Information Security Policy](#)
- [Records Management Policy](#)

11. Further information

For further advice on records management or managing emails please contact the [Governance Adviser \(Records Management\)](#) in Governance Services.

For advice on the technical aspects for managing your email, please contact the IS Service Desk, email: ISServiceDesk@napier.ac.uk, telephone: +44 (0)131 455 3000

The following links provide further information and guidance:

11.1 Information Security Policy: Email and Internet Use

Section 9 of the Information Security Policy for Users specifically refers to the use of email:

<http://staff.napier.ac.uk/services/cit/Documents/Security/Information%20Security%20User%20PolicyV2.0.pdf>

9. Email and Internet Use

This section defines the regulations to ensure secure use of email and the internet.

1. Always check the address line before sending a message and check it is being sent to the correct person (one of the most common forms of alleged security breaches).
2. Never represent yourself as another person or persons
3. Delete electronic mail messages when they are no longer required.

4. Take care not to express views, which could be regarded by others as offensive or libellous. Comments made in jest may be misinterpreted by the recipient. In a case of harassment it is the effect of a communication on the recipient that is considered and not the intention of the sender.

5. Any personal private emails must be saved in a separate folder from work related emails. Clearly mark all emails that are of a personal nature as “personal”

6. Personal/private postings to wikis, blogs, newsgroups or similar referencing Edinburgh Napier University must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Edinburgh Napier University.

7. Users must not open e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code or any other form of Malware.

8. Do not forward electronic mail messages to other individuals or groups that have been sent to you containing personal data (as defined by the Data Protection Act 1998) without the permission of the originator.

9. Do not participate in chain or pyramid messages or similar schemes.

10. Do not unnecessarily send excessively large electronic mail messages or attachments.

11. The University network and the internet connection are not to be used for peer to peer file sharing except with the permission of the Head of Information Services

12. Report any unusual or suspect email messages or network activity to the IS Service Desk.

If there are any questions regarding any of these regulations contact the IS Service Desk by emailing ISServiceDesk@napier.ac.uk or telephoning extension 3000.

11.2 Electronic Information Security Policy: Monitoring and Logging

The scanning and monitoring of University email accounts by Information Services is detailed in the following policy:

<http://staff.napier.ac.uk/services/cit/Documents/Security/Information%20Security%20Monitor%20and%20Log%20V3.pdf>

2. Monitoring

Networks and computers may be monitored and usage logged...During monitoring, information may be examined, recorded, copied and used for authorised purposes. All

24

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

information, including personal information, placed on or sent over this system may be monitored. Monitoring is automated in the detection and removal of viruses, malware, spam, pornographic and inappropriate URL's and other activities not lawful to University business. Use of the Edinburgh Napier University information technology, authorised or unauthorised, constitutes consent by the user to monitoring of these system. Unauthorised use (as outlined in the Electronic Information Security Policy Statement and associated policies) use may give rise to disciplinary procedures or criminal prosecution. Evidence of unauthorised use collected during monitoring may be used subsequently in a disciplinary, criminal or another form of proceedings. Use of the Edinburgh Napier University IT systems constitutes consent to monitoring for these purposes.

3. Email Scanning

Incoming e-mail may be scanned by Edinburgh Napier University including using virus-checking software. The software may block unsolicited marketing e-mail (spam), e-mail which has potentially inappropriate attachments, bad language or any other inappropriate material. If there is a suspected virus in an e-mail the sender will automatically be notified and you may receive notice that the e-mail is not going to be delivered to you because it may contain a virus

11.3 Email Security Guidance

Information Services have a dedicated intranet page giving guidance on email security:

<http://staff.napier.ac.uk/services/cit/infosecurity/Pages/EmailSecurity.aspx>

The screenshot shows the Edinburgh Napier University Staff Intranet. The header includes the university logo and navigation links like 'Schools', 'Service Depts', 'University Groups', 'News', 'Email', 'My Workplace', 'Staff Directory', 'Quick links', 'Service Status', and 'iPoint'. The main content area is titled 'Information Services' and features a breadcrumb trail: 'YOU ARE HERE: Edinburgh Napier Staff Intranet > Service Depts > IT > Information Security > Staying Safe when using Email'. A left-hand navigation menu lists various security topics. The main article, 'Staying Safe when using Email', explains that email is a common route for attacks and lists protective measures: free anti-virus and anti-spyware software, an automated email protection system, and ensuring all machines have anti-virus and anti-spyware installed. It also includes a 'Frequently Asked Questions' section with a question about phishing emails and an answer explaining that phishing emails ask for personal information like passwords or bank details.

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive. (NOT the H: Drive, C: Drive or MySite – these are not shared)

11.4 Data Protection Code of Practice: Email and Personal Data

Further guidance on emails containing personal data see:

<http://staff.napier.ac.uk/services/governance-compliance/governance/DataProtection/CodeofPractice/Pages/default.aspx>

7.5 Transfer of Personal Data

7.5.1 All transfers of personal data are to be authorised and/or conducted at an administrative or managerial level appropriate to the type of personal data being transferred and carried out in accordance with any applicable data transfer agreement. Data is only to be transferred in secure conditions which are commensurate with the anticipated risks and appropriate to the type of personal data involved.



7.5.2 Key points to note are:

- It must **not** be assumed that documents transferred by electronic means e.g. email, web transfers, File Transfer Protocol are secure
- Material containing sensitive personal data, or data that if it should be lost is likely to cause damage or distress to the subjects should always be encrypted to an appropriate standard before it is transferred
- Staff must consider whether data can be anonymised before it is taken off University premises and/or sent either by post or courier
- If this is not possible and it is deemed absolutely necessary to download personal data to physical devices e.g. USB memory sticks, CDs or DVDs then the data **must** be encrypted.
- Hardcopy data should also be transferred in a manner proportionate to its sensitivity

Information Services publish [guidance on data encryption](#) and the software to be used.

A staff  [checklist on Security of Personal Information](#) is available for summary reference purposes.

9.3 Internet and Intranet Monitoring

The University requires the ability to inspect all data held on its computer equipment and to inspect all email and other electronic data entering, leaving or within the University network to ensure conformity with:

- The University's Information Security Policies
- Contractual agreements with third parties
- UK legislation

Further guidance is in the University's  [Monitoring and Logging Policy](#).

11.6 Method of Transferring Personal Data

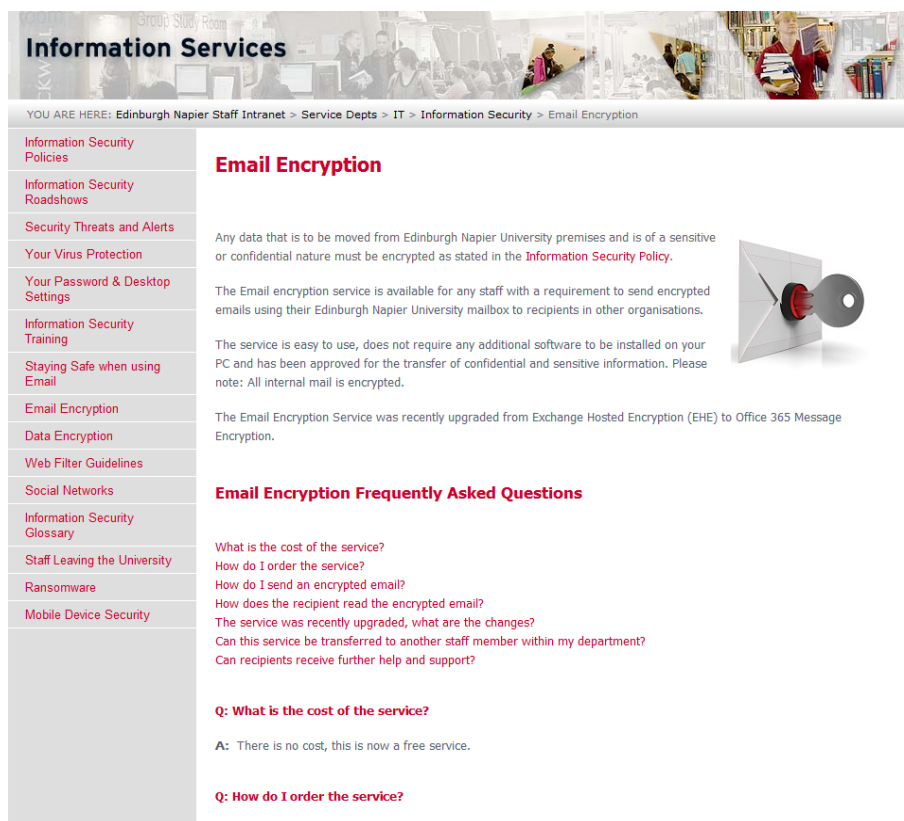
Where it has been established that personal data may be transferred, this should be done in accordance with [section 7.5](#) of this Code of Practice; electronic transfers of personal data must be encrypted. IT Services provide guidance on both [Data Encryption](#) and on [Email Encryption](#).

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

11.5 Email encryption information and guidance

Email encryption is very easy to use and set up – IS have an intranet page which gives more information and can be accessed here:

<http://staff.napier.ac.uk/services/cit/infosecurity/Pages/EmailEncryption.aspx>



The screenshot shows the 'Information Services' intranet page. At the top, there is a navigation breadcrumb: 'YOU ARE HERE: Edinburgh Napier Staff Intranet > Service Depts > IT > Information Security > Email Encryption'. A left-hand menu lists various security topics, with 'Email Encryption' highlighted. The main content area is titled 'Email Encryption' and contains several paragraphs of text. The first paragraph states that sensitive data must be encrypted according to the Information Security Policy. The second paragraph explains that the service is available for staff needing to send encrypted emails to other organizations. The third paragraph notes that the service is easy to use and approved for confidential information. The fourth paragraph mentions a recent upgrade from Exchange Hosted Encryption (EHE) to Office 365 Message Encryption. Below this is a section for 'Email Encryption Frequently Asked Questions' with several questions and answers. An image of a keyhole and a key is positioned to the right of the main text.

Information Services

YOU ARE HERE: Edinburgh Napier Staff Intranet > Service Depts > IT > Information Security > Email Encryption

Information Security Policies

Information Security Roadshows

Security Threats and Alerts

Your Virus Protection

Your Password & Desktop Settings

Information Security Training

Staying Safe when using Email

Email Encryption

Data Encryption

Web Filter Guidelines

Social Networks

Information Security Glossary

Staff Leaving the University

Ransomware

Mobile Device Security

Email Encryption

Any data that is to be moved from Edinburgh Napier University premises and is of a sensitive or confidential nature must be encrypted as stated in the **Information Security Policy**.

The Email encryption service is available for any staff with a requirement to send encrypted emails using their Edinburgh Napier University mailbox to recipients in other organisations.

The service is easy to use, does not require any additional software to be installed on your PC and has been approved for the transfer of confidential and sensitive information. Please note: All internal mail is encrypted.

The Email Encryption Service was recently upgraded from Exchange Hosted Encryption (EHE) to Office 365 Message Encryption.

Email Encryption Frequently Asked Questions

What is the cost of the service?
How do I order the service?
How do I send an encrypted email?
How does the recipient read the encrypted email?
The service was recently upgraded, what are the changes?
Can this service be transferred to another staff member within my department?
Can recipients receive further help and support?

Q: What is the cost of the service?

A: There is no cost, this is now a free service.

Q: How do I order the service?

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

11.6 General Outlook email information and guidance

IS have an intranet page which gives guidance, information and hints and tips on how to use Outlook, which can be accessed here:

<http://staff.napier.ac.uk/services/cit/StaffEmail/Pages/StaffEmail.aspx>

The screenshot shows the Edinburgh Napier University Staff Intranet page. At the top, there is a search bar, a 'Logout' button, and a welcome message: 'Welcome to the Staff Intranet'. The Edinburgh Napier University logo is on the right. A red navigation bar contains links for Schools, Service Depts, University Groups, News, Email, My Workplace, Staff Directory, Quick links, Service Status, and iPoint. Below this is a banner for 'Information Services' with a background image of students in a library. A breadcrumb trail reads: 'YOU ARE HERE: Edinburgh Napier Staff Intranet > Service Depts > IT > Staff Email'. A left-hand menu lists various services, with 'Staff Email' selected. The main content area is titled 'Your Email' and contains the following text: 'Each staff member at Edinburgh Napier University is supplied with a **Microsoft Outlook** email account, hosted on **Microsoft Exchange**, and is allocated **1GB** worth of storage space within their email accounts.' Below this is a blue box with the Office 365 logo and the text 'Coming Soon - Office 365 for staff members...'. Further down, it says 'This page provides help using Microsoft Outlook.' and 'You may also find the following pages useful:'. A list of links includes 'Email Security', 'Email Encryption', 'Remote Access to Email', and 'Mobile Devices (includes information on setting up your device to access University email)'. A note states: 'For guidance on managing email records please refer to [Governance Services Email Management intranet page](#).' At the bottom of the main content area, there is a section titled 'About Microsoft Outlook'.

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive. (NOT the H: Drive, C: Drive or MySite – these are not shared)

Email FAQs

Why do I need to save email records on a shared drive?

Have you ever found yourself trawling through your email looking for information or having to ask a colleague for something which is in their email?

1) Saving all the records (or as many as possible) in one place where (a) the appropriate colleagues have access, and (b) the emails are saved with other records relating to the same business, makes them easier to find and available to those who need to refer to them. The filing structure for the department in the shared network area should be logically set up to reflect the functions and activities of the department, and to take into account the retention periods for the records (and any other information). Keeping records in your email account makes them available **ONLY TO YOU**, and although they may be easy for you to find using the various sort and search facilities, this is reliant on your individual knowledge of who sent the email and when it was sent, etc. Email (and any other records) received or created by you in the course of your employment with the University belong to the institution and it is your responsibility to ensure that they are managed appropriately.

How long do I keep emails?

There is no specific retention period relating to emails, per se, as it is the content of the email **not** the format which is important. You shouldn't have many emails older than 6 months in your email account and certainly none older than 12 months – they should be saved on a shared network drive or have been deleted once there was no longer a business requirement to keep them.

1) Records – if the email is evidence of University business then it should be stored in SharePoint or the S: Drive along with other records related to the same business (and will therefore be destroyed/deleted along with those records in due course according to the corresponding [Records Retention Schedule](#))

2) Copies of emails sent to others/attachments – it is the responsibility of the originator to ensure that these are stored appropriately if they are University records, therefore you can delete them once they have served their purpose. If you are still using them as reference material please see the guidance referring to reference material below.

Attachments - ideally, the originator should supply you with a link to the file rather than sending the file as an attachment as this means that there will be a proliferation of copies of the same file saved in various locations on the University network and version control becomes difficult. SharePoint is ideal for storing files which need to be accessed by numerous people and has built in version control and excellent collaboration capability.

3) Reference material – generally try to delete reference material as soon as you have read it. If the email/s are reference material with ongoing value save them in SharePoint or the S: Drive along with other records related to the same business.

Putting them in a folder entitled 'reference material' will make it easier to find them for use while they are required and categorises them for easy deletion once they are no longer required.

4) Ephemeral/Transitory Records –are those which are only of value short-term. If there is provision for these within your departmental retention schedule then refer to that, however it may be necessary to use your own judgement e.g. meeting invitations and other information pertaining to the meeting are unlikely to be of any use once the meeting has concluded and the minutes circulated. Reference material is unlikely to be needed once the purpose for which it was retained has been finalised (it may be referenced in the final document/s).

5) Emails retained for your personal evidence that you requested something or something was requested of you must be stored in such a way that you can routinely reassess them and decide whether or not to continue storing them. Best practice is to store all University records in a shared area on the network drive, for instance, if you deal with procurement for your department and are keeping email requesting purchases as 'evidence' these could be stored with related information for that year in a shared network area. The value of the request may have a bearing on its retention as may the reason for the purchase (e.g. project) – please contact the [Governance Adviser \(Records Management\)](#) if you have any specific retention period queries.

Can emails form a contractual undertaking?

Yes, they can, so ensure that you are authorised to enter into the agreement or contract prior to doing so – particularly where an external party is involved.

Is any email/Outlook guidance available?

Yes, guidance and information is available on the IS intranet pages:
<http://staff.napier.ac.uk/services/cit/StaffEmail/Pages/StaffEmail.aspx>

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

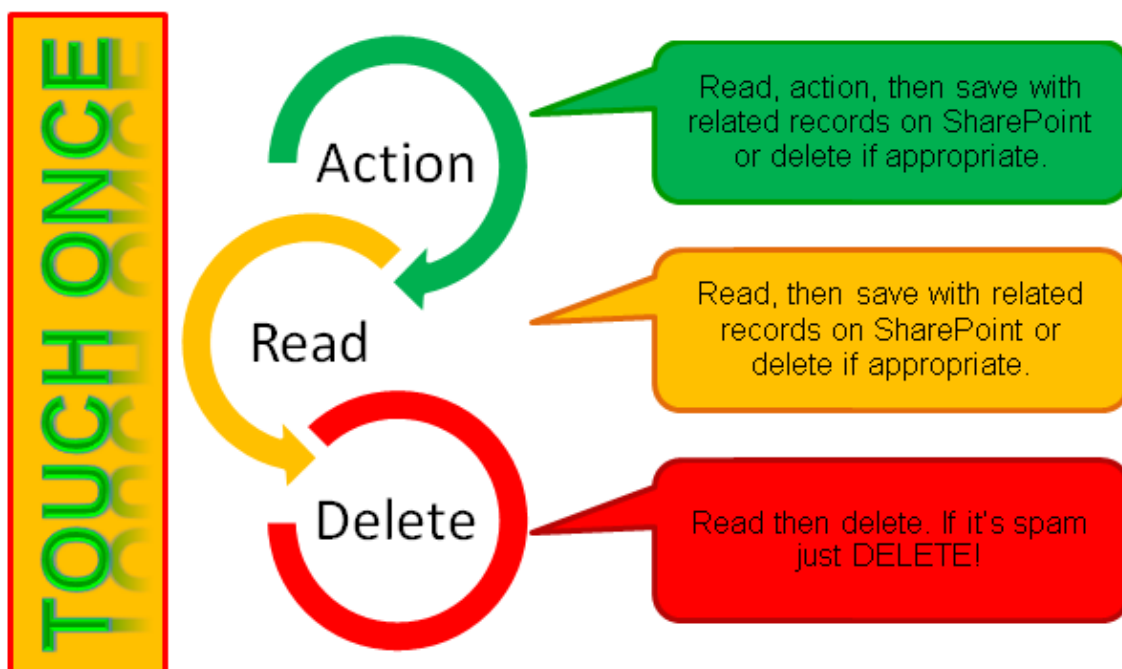
Strategies to avoid email overload

- If you don't really need to send an email, pick up the phone and speak to a colleague rather than emailing – this cuts out at least one email out & one in.
- Have folders set up in SharePoint or the S:Drive ready to receive those emails that are 'records' or reference documents
- 'Touch once' time management strategy - try to deal with as many emails as you can as soon as you have read them (including actioning, filing/deleting them). If it will take less than 3 minutes to respond, then do so! This saves coming back and having to read it again.

'Action' emails are those containing a request for action or information and may also include those providing a response to a request you have sent.

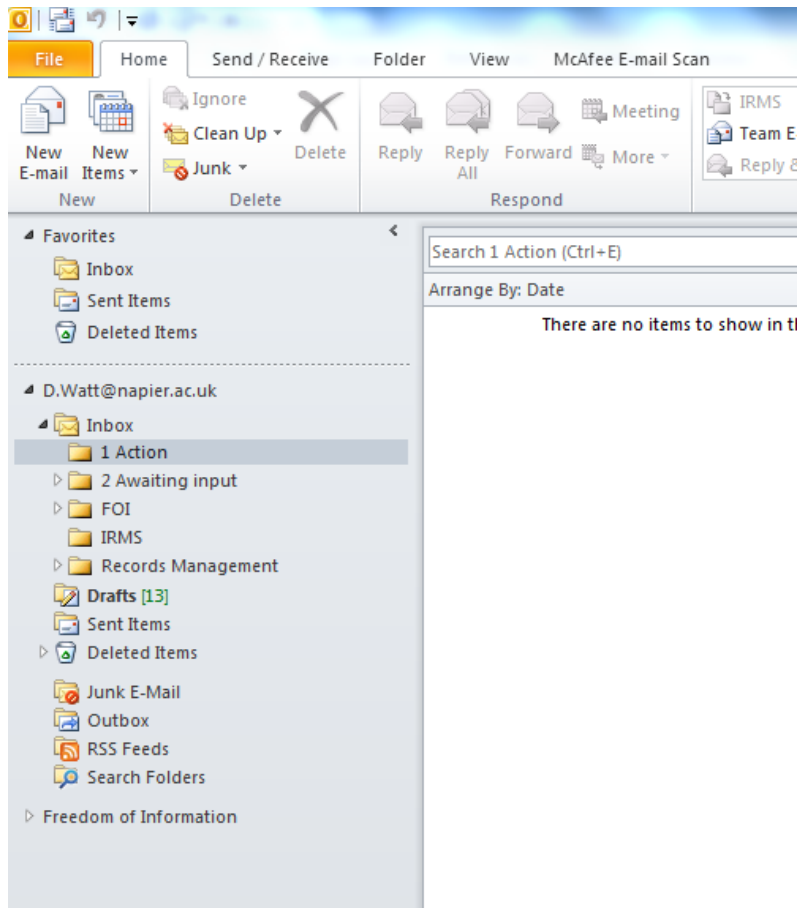
'Read' emails are those received for your information only and more likely to be those providing a response to a request you have sent, or message for reference only e.g. from a listserv, or newsletters, office information, etc.

'Delete' emails include some that you read then delete and junk or spam mail which you just delete.



For those emails that cannot be dealt with in 3 minutes, or require input/action from another person before they can be dealt with consider setting up folders to put these into which will assist in keeping your inbox clear and making it easy to find those that still require work, as per the example below:

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)



Don't use your 'Inbox' as your 'To DO' list.

- If you are regularly asked for the same information then consider setting up a SharePoint site to make this information available to the necessary people, and then they can go directly to the information rather than asking you.
- Unsubscribe from email alerts and lists that you don't have time to read
- Give yourself some reply timescales and set up a template acknowledgement for those which will need further work and may require a longer response time.
- Set time aside to reduce the number of emails in your inbox. You may find it helpful to set up an 'appointment' for yourself in your calendar to do this.
- Email free time – during time set aside for emails or at other times when you are busy with other work you could also set up an automatic response message letting people know that you are busy and asking them to contact you by phone if it is urgent. *Please check with your manager* if you are intending to have email free time as this may *not* be possible in some teams.
- Turn off email 'toasties' (pop up messages informing you that you have received an email) to minimise interruptions, and have set times during the day to check your email. You could set up an automatic response to inform recipients of the times you will check your email and asking them to contact you by phone if it's urgent. *Please check with your manager before doing this.*
- Delegate work if appropriate
- Set up rules and filters as/if appropriate

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

- Keep your work and personal emails separately. Do not use non-University email accounts to conduct University business – doing this does NOT mean that these communications fall outside the remit of the information legislation. *Any* email sent or received in the course of University business is subject to the governing legislation.
- Don't be an email 'hoarder' – sifting through reams of emails trying to remember who sent you what email when *wastes time!* It's just an electronic version of the desk pictured below...



Image – Edinburgh Napier Health and Safety Team

'Shared network area' refers to SharePoint libraries/folders (preferable) and shared or departmental network areas such as the S: Drive.
(NOT the H: Drive, C: Drive or MySite – these are not shared)

Index

- 'Out of office' message, 21
- absent staff, 22
- access, 7, 8, 14, 19, 21, 22, 29
- Access, 7, 15
- accessible**, 4, 11, 22
- accountability, 10
- Action**, 31
- active owner, 22
- activities, 11, 25, 29
- Addressing messages, 16
- attachments, 14, 19, 24, 25, 29
- auditable trail, 16
- Auto-Complete, 7
- automatic response, 32
- business activity, 8, 10
- business and regulatory requirements, 11
- business process, 12
- business processes, 12
- business related activities, 9
- business transaction, 10
- categorisation, 8
- changing roles, 22
- collaboration, 19, 29
- communication tool**, 4
- compliance, 9, 10, 11
- composing, 16
- confidential, 7, 8, 14, 16, 20
- content, 12, 16, 19, 29
- Content and tone, 16
- contractual undertakings, 10
- contractually binding agreements, 16
- conventions, 10, 12, 13, 16
- conversations, 7, 19
- Creating and replying to messages, 15
- data breaches**, 4
- Data Protection Act 1998, 24
- Data Protection Code of Practice, 15, 26
- decision, 9
- decisions, 4, 7, 9, 10, 16
- Delete**, 14, 22, 23, 31
- disciplinary, 4, 25
- discriminatory, 17
- duplicate, 11
- Email accounts of leavers, 22
- Email attachments, 19
- Email encryption information and guidance, 27
- Email FAQs, 29
- Email Policy, 2
- Email Scanning**, 25
- encrypted, 12, 16
- evidence, 4, 7, 9, 12, 29, 30
- exceptions, 10
- external, 10, 11, 17, 30
- File, 11
- filing structure, 9, 12, 29
- filing structures, 11
- filing systems, 11
- flags, 16, 20
- FOISA, 4
- generic departmental email accounts, 9
- generic email account*, 21, 22
- generic email addresses, 22
- generic mailboxes, 22
- heading, 15
- hints and tips, 28
- historical value, 9
- hyperlink, 19
- important points, 4
- individual responsibility*, 4
- Information Commissioner's Office, 4
- Information Security Policy, 23
- intercepted, 7
- IS guidance**, 7
- keep, 4, 8, 10, 11, 20, 29
- legally admissible, 12
- legislation**, 4, 7, 14, 33
- Legislation, 4
- Managing your inbox, 20
- mobile devices, 7
- Monitoring and Logging, 24
- multiple recipients, 10, 11
- naming conventions, 12
- newsletters, 10, 31
- Non-record, 10
- official 'records', 4
- operational, 9, 10
- out of office, 21, 22
- performance and technical issues, 20
- permissions, 8
- personal**, 4, 7, 8, 14, 15, 16, 21, 22, 23, 24, 25, 26, 30, 33
- Personal, 4, 7, 9, 10, 20, 23, 24, 26
- Personal Correspondence**, 9
- personal data, 7
- Personal data disclosures, 4
- policy, 7, 9, 10, 12, 14, 24
- Prefixes, 16
- punctuation, 17

Read, 14, 31
 record, 7, 8, 9, 10, 11, 12, 14, 15, 19, 20, 22
 records, 4, 7, 8, 9, 10, 11, 12, 14, 15, 16, 19, 22, 23, 29, 30, 31
Records, 2, 4, 7, 8, 9, 10, 11, 13, 29, 30
 RECORDS, 4, 9
 Records Retention Schedule, 8, 29
 records retention schedules, 9
 reference material, 9, 29
 reference purposes, 10
 related records, 8, 11, 12, 14
 reply all, 16
 Responsibility, 10
 restricted, 8
 retention, 4, 8, 9, 11, 29, 30
 retention period, 8, 29, 30
retention periods, 4, 8, 29
 retrieval, 12, 22
risk, 4, 7, 14, 19, 20, 22
 Routine Management, 7
 Scottish Information Commissioner, 4
 scrutiny, 14, 17
 secured folder, 7
 Security, 2, 7, 16, 17, 21, 23, 24, 25
 sender or initiator of the dialogue, 10
 sensitive, 7, 8, 14, 15, 16, 20
 sensitive information, 7, 20
 shared network area, 7, 11, 12, 15, 16, 19, 22, 29, 30
 slow system response times, 20
 smart phone, 7
Spam, junk, unsolicited or suspicious messages, 9
 storage requirements, 20
 Strategies to cope with the influx of email, 31
 strings, 19
 Structure and grammar, 17
 subject, 4, 9, 12, 13, 14, 15, 16, 17, 19, 20, 23, 33
 Subject, 15
 technical errors, 22
 template acknowledgement, 32
 title, 12, 13, 15, 19
 title ('subject'), 12
 toasties, 32
 unencrypted emails, 7
 wrong recipient, 7

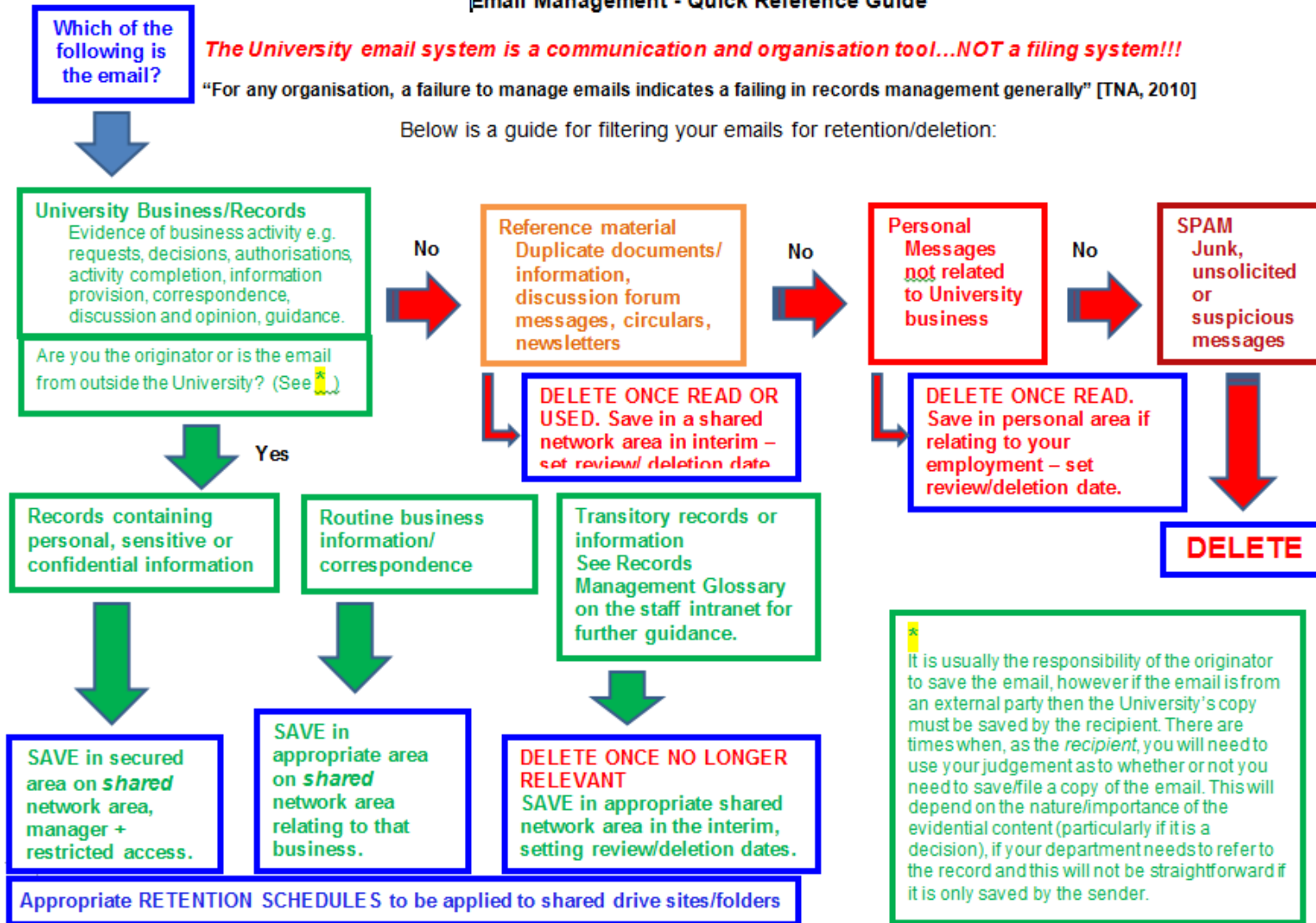
APPENDIX A – Quick Reference Guide

Email Management - Quick Reference Guide

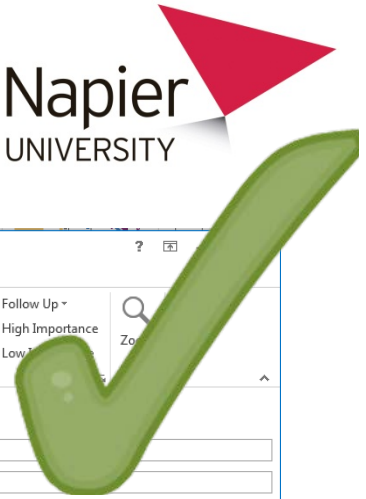
The University email system is a communication and organisation tool...NOT a filing system!!!

“For any organisation, a failure to manage emails indicates a failing in records management generally” [TNA, 2010]

Below is a guide for filtering your emails for retention/deletion:



APPENDIX B – Simple Steps to Effective Business Emails



Describe topic briefly for maximum impact and to facilitate filing - Message (HTML)

FILE MESSAGE INSERT OPTIONS FORMAT TEXT REVIEW

Send Attach and File Items Attach File Attach Item Signature

From: Governance & Planning

To: Only include those who NEED to be included

Cc: Consider subsequently forwarding the message AND stating if it is for 'information' OR 'action'.

Bcc: Avoid using this - consider forwarding as above (see * for group emails)

Subject: Describe topic briefly for maximum impact and to facilitate filing

- 1) Get to the **main/most important point** early on, including any requests for **action**. Advise if there is a **timescale**.
- 2) **One topic** per email makes the email easier to deal with and file.
- 3) Use **appropriate language** – emails about *University business* are subject to information legislation and may be disclosed (FOISA/DPA) and/or monitored.
- 4) Keep emails **brief** – don't write a voluminous essay which is time consuming and difficult to decipher.
- 5) Consider if email is the best form of communication – would a phone call or meeting be more appropriate and efficient than a string of emails?
- 6) Consider using a standard/formal template if your email is an inter-office memo, letter, etc.

Kind regards,

(Signature)
Name
Job Title
Department
Address and contact details
(Providing a phone number may reduce subsequent emails)

* There are occasions when the Bcc function should be used if sending out a group email to protect the privacy of recipients – see detailed guidance on the intranet

URGENT!! Subject: EVERYTHING!! - Message (HTML)

File Message Insert Options Format Text Review

Attach File Attach Item Signature

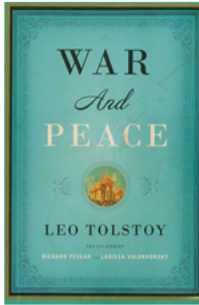
From: Governance & Planning

To: Everyone

Cc: All Managers

Bcc: Secret Mailing List

Subject: URGENT!! Subject: EVERYTHING!!



Personal messages
Unprofessional/derogatory comments
Third party personal data

Regards,
Name and no contact details

☒ Cc...Disseminating responsibility? Asking for action? Providing information? Consider 'forwarding' the email and making this clear.

☒ URGENT – don't mark everything urgent or flag as 'High Importance' – use this only when necessary/appropriate.

