

EMAIL MANAGEMENT

INFOKIT



www.jiscinfonet.ac.uk/infokits/email-management

Email Management	4
The rise and rise of email.....	4
The Risks Associated With Email	4
Creation	5
Ensuring Appropriate Email Use	6
Appropriate Use Policy	6
Making Staff Aware	7
Enforcement	7
Encourage Staff To Create Fewer Emails	7
Providing And Promoting Alternatives.....	7
Promoting Good Practice	8
Improving Your Email.....	8
Titles & Other Metadata	8
Content	8
Email Disclaimers	9
The Case 'For' Disclaimers	9
The Case 'Against' Disclaimers.....	9
Active Use.....	9
Monitoring Email Use.....	10
Remote/Home Use Of Email.....	10
Outsourcing Your Email Provision	11
Email Security	12
Passwords & User Behaviour.....	13
Account Maintenance.....	13
Making Best Use Of Your Email Software	13
Semi-Active Use	14
Identifying Emails As Records	15
Next Steps.....	15
Managing Emails As Records.....	16
Authenticity	16
Completeness.....	16
Reliability	16
Fixity	16
Managing Email Retention.....	16
By What Criteria Should Email Retention Be Decided?.....	17
Retention Based On Content	17
Separating The Wheat From The Chaff	17

Managing Email Retention In Context	17
What Happens When A Member Of Staff Leaves?.....	18
Finding Emails.....	18
The Advantage Of Central Storage.....	18
User Behaviour During A Legal Discovery Exercise	19
Final Outcome	19
Archiving & Preserving Emails.....	19
Deleting Emails	20
Has Your Deleted Email Really Gone?	20
Disclaimer	22

Email Management

The rise and rise of email

Sending messages via electronic communication has a longer history than is commonly thought, pre-dating the internet and stretching back to the 1960s. However, it was with the advent of the World Wide Web during the 1990s that email as the business and social phenomena that it is today really took off. It is difficult to obtain accurate figures for the number of emails being sent at any one time but calculations in 2003 suggested a staggering figure of 31 billion emails were being sent each day with a prediction that that figure was set to double by 2006 (see the [Executive Summary](#) from How Much Information? 2003).

Regardless of the precise figures it is true to say that email has revolutionised business communication in a way second only to the introduction of the telephone and is indeed rapidly supplanting the phone as the method of communication of choice for many workers. It is now a common occurrence for an office worker to have to process in excess of 50-60 emails each day. Some of these may contain valuable information or represent important steps in the conduct of a business process; whilst others may be of fleeting or no use at all - or worse nothing more than spam designed to extort money or spread viruses. Email is now also integrated into other forms of business information - whether being used to transfer documents, co-ordinate diaries, or keep track of project milestones.

It is not hard to see why email use is so widespread. Its ease of use has helped form its own informal style which makes writing an email far quicker than composing a letter. The same message can be easily sent to as many people as you want at the same time and you can be sure that it will be received within minutes of sending it, compared with the days taken to receive post via 'snail mail'. And best of all of course it is free (at least so far as the end user is concerned). Whilst some of these advantages could also be claimed by the humble telephone, email has the added benefits to the sender of not requiring the recipient to be available at the time that he/she wants to communicate; whilst to the recipient they can choose to respond at the time that suits them as well as providing a useful written source to refer back to at a later date.

It's true that some new kids on the block are emerging which may over time challenge the dominance of email, especially the growing trend for 'instant messaging' solutions and [VOIP](#), but it will be some time before they topple email from the number 1 spot. The rise of wireless technology and mobile devices mean it is now as easy for users to send and receive email whilst out of the office as it is when sat at their desk - further adding to the convenience and usability of email and hence contributing to the ever increasing numbers sent.

The Risks Associated With Email

Unfortunately it is not all good news when it comes to email, and paradoxically many of the advantages listed in the previous section are also largely responsible for the considerable risks associated with its use.

Its ubiquity and flexibility mean that email is routinely used for an astonishingly wide variety of purposes, some of which are outlined in the table below

Table below - Range of functions email is regularly used for

Sharing information	Sharing documents	Asking questions
Requesting information	Planning social events	Agreeing a course of action

Sharing jokes/gossip	Holding discussions	Swapping contacts
Planning business meetings	Confirming agreements	Assigning tasks

This mixture of formal and informal, business and social, serious and frivolous is a dangerous mix. The eyes of the law may be unable or unwilling to distinguish between them leaving every single email sent or held by your institution as part of its auditable information holdings. With all colleges and universities now subject to the [Freedom of Information Act](#) the question staff need to ask themselves is: 'would I be happy for the contents of my email to be printed in the local newspaper'? The answer is likely to be a resounding 'no'. This is because people have become accustomed to treating emails as ephemeral without regard for the evidential trail they leave behind. There are countless examples of users who have fallen into this trap only to find their flippant, off the cuff remarks used against them as evidence of libel, discrimination or abuse.

Nor is this a risk faced solely by the individual staff concerned. The institution itself may well find itself liable for the transgressions of its staff - especially if it is unable to demonstrate that it is taking an active approach to encouraging good practice and managing email use.

The ease of email creation and distribution, combined with the sheer volume of messages that staff are expected to deal with also leads to inevitable problems. Messages containing sensitive content are all too easily sent to the wrong person who just happens to share a similar name to the intended recipient, whilst confidential information is often to be found inadvertently buried at the bottom of a long chain of forwarded messages.

Without regular, ongoing management by the user their email account will rapidly become an untamed and apparently untameable monster. Inboxes containing literally thousands of messages are not uncommon and many people have developed a way of working which relies on the kaleidoscope of information their inbox contains as an apparently indispensable 'electronic memory'. Whilst there may be some value to the user in this approach (though probably less than they imagine) it also results in considerable costs and risks to the institution. As well as the dangers resulting from inadvertently keeping 'dangerous' information, it is also often the case that information of value to a number of functions within the institution remains locked away within this inaccessible data silo and reliant on the vagaries of individual practice for survival.

Creation

Both email as a format and the functionality of the applications used to create them contributes largely to the problems associated with their management. Most aspects of email technology and functionality are weighted in favour of the sender and as a result work against the interests of the recipient. For example the ease, speed and cheapness of their creation and distribution mean little or no forethought or consideration is required. There are no practical barriers or costs associated with creation which might cause the potential sender to pause and think twice before creating yet another message.

Until recently this has seemed a relatively trivial issue. Users may individually struggle to cope with the volume and variety of messages they receive but the associated costs and risks to the institution as a whole were largely ignored. Now, with email servers containing terabytes of data the costs associated with storage and maintenance are no longer trivial. Furthermore institutions are beginning to realise the hidden costs and dangers associated with uncontrolled email creation - not least the risk of dangerous and damaging information coming to light as part of a response to a Freedom of Information Act request or other legal discovery exercise.

Many institutions are rapidly coming to the conclusion that email management can no longer be left to individual members of staff to perform on a 'best efforts' basis and that a more proactive and co-ordinated approach is needed. The purpose of this strand of the Managing the Information

Lifecycle infoKit is to outline the main elements which need consideration as part of such an approach. In particular looking at how a combination of three main elements; technology, policies/procedures, and user training need to be considered in unison to achieve an effective, institution-wide response.

The contents of this section build on and augment the information provided in the Information Lifecycle - Creation strand and should be considered in this light. What this section attempts to do is build on the general good practice guidance on information creation covered previously and look specifically at the additional requirements for creating good emails.

As such it will be of use to those tasked with managing and maintaining email services within the institution and those with an interest in the management of information and records.

The topics covered within this section include:

- Ensuring appropriate email use
- Encouraging staff to create fewer emails
- Encouraging staff to create better emails
- Email 'disclaimers'

Ensuring Appropriate Email Use

As we have already seen, the flexibility of email has led to a user culture where email is routinely used for a variety of formal and informal purposes. It is therefore vital that the institution clearly defines what is and isn't 'acceptable use' of email and that users are informed of the distinctions.

Appropriate Use Policy

Formulating an email appropriate use policy provides an essential cornerstone of this strategy. Without a clear definition of what is and isn't acceptable the institution will not be able to demonstrate that responsibility for any breaches of the law rests with the individual and not the institution. It is also less likely that the institution will be able to take punitive measures against any staff found using email inappropriately.

Some categories of inappropriate content/use will be easier to define than others. The table below includes categories of email which will need consideration when formulating an appropriate use policy - whether they are deemed 'inappropriate' will, in some cases, be dependent upon local circumstance. As the table below makes clear, inappropriateness might equally be judged according to whether email is considered the safest, most appropriate format for transferring what is actually perfectly 'legitimate' content.

Table below - categories of email content which may be deemed inappropriate

Category	Examples
Malicious	Viruses, worms, Trojans etc.
Illegal	Pornography, terrorism/extremism, libellous
Offensive	Sexist, racist, harassment, bullying

Sensitive personal data	Disciplinary matters, health/medical information etc.
Commercially sensitive data	Financial information, contractual negotiations, intellectual property
Personal use	Online shopping, gossip, arranging social life, etc.

Making Staff Aware

It is an important first step to formulate what is and isn't acceptable use into a policy, but this alone is not sufficient. The most obvious additional requirement is that staff are informed and regularly reminded of the policy and its contents. The policy should be endorsed by senior management and distributed to all users bearing this official endorsement. Including it as part of induction packs for new starters will ensure all new staff also receive it. Its content should form part of any IT user training (e.g. as part of Introduction to Outlook courses) and links to it should be provided from the institution's webmail service home page and the intranet.

Enforcement

Breaches of the policy should be stated as a disciplinary offence and potential grounds for dismissal within staff contracts. Consideration should also be given to internally publicising breaches of the policy and any measures taken as a warning to others.

Encourage Staff To Create Fewer Emails

Given that a large percentage of the emails received by staff within your institution will have been created internally, reducing the number of emails individual staff send will subsequently reduce the number of messages all staff receive and need to manage. This will not only help reduce the overall volume of network traffic and decrease the chances of mistakes through user-error, it will also increase the overall efficiency of your institution. Many users will instinctively break off from the task in hand when notified that a new message has been received, thus breaking their train of thought. Also, if you assume an average of 2 minutes is spent reading and responding to each message, multiplying that by the average number of messages received and then by the number of staff in your institution it is possible to quickly arrive at a frighteningly high staff-costs figure.

Providing And Promoting Alternatives

In order to try to wean users of sole reliance on email it is necessary for the institution to provide and promote alternatives. That way email can be seen as representing just one tool amongst many at the user's disposal for use only when it makes sense to select it. Remind users that one quick phone call can save a dozen emails when trying to arrange a meeting and support this by ensuring that the internal phone directory is easy to find and up-to-date and that staff have access to modern phones which can store frequently used numbers etc.

The institution should also ensure efficient use of its intranet to distribute 'all staff' information, perhaps making use of RSS feeds to notify users of updates and changes. It should also ensure that all staff have access to shared file areas to prevent the need to rely on email to share documents (this also has additional information and records management advantages explored in [version control](#) from the Records Management strand).

Promoting Good Practice

A combination of documented procedures and user training will make a significant difference. These should not only cover when not to use email as outlined above, but also more detailed guidance on thinking carefully before selecting 'Reply All' or when sending emails to large groups of users. The institution should ensure that it practices what it preaches in this regard as the high volume of 'All staff' emails used to transmit information of use to only a very small, easily identified, group of users is often a common culprit!

Some organisations have gone even further and instituted regular 'no email days' when it is forbidden (or at least strongly frowned upon) to send or respond to internal emails. Such initiatives, even if promoted as one off events can help raise the profile of the problem, remind users of the alternatives and help them recall the advantages of an un-interrupted period of work.

Publishing statistics on the volume of emails sent by the institution's servers each day/week/month and setting a reduction target can also be an effective way of raising awareness - especially if accompanied by a small prize for the team or department which manages to meet the target figure first.

Improving Your Email

There is little that can be done from the technical or system perspective to encourage staff to create better emails. Any improvements in this regard are likely to be largely dependent on the same blend of procedures and user training referred to in the previous section.

Once again, the focus is on changing the behaviour of the sender to make life easier for the recipient and thus helping to initiate a virtuous circle of improved management. Poorly drafted emails described by unhelpful (or absent) titles and accompanied by indiscriminate use of message status indicators are not only annoying to receive but add considerably to the daily burden of trying to manage email. They also increase the risks of damage to the institution's reputation and legal interests through the amplified likelihood of mistakes caused by poor management and the transmission of inappropriate material.

Titles & Other Metadata

The only user generated metadata routinely added to an email is the subject heading or title. As such it is important that the user is made aware of the value of attaching good, clear and unambiguous titles to all their messages. Ideally the title should be clear enough for the recipient to know the basic content of the email and its context prior to opening the message. Particular attention should be paid when the content of a thread of messages changes over time and starts to have little or nothing in common with the original title. The default options within your email application should be checked to see whether it is possible to prevent messages being sent where the subject header has been left blank.

The use of message status indicators can be helpful to provide an immediate indication to the recipient of whether an email is urgent or of low importance. Users should be encouraged to use these sparingly (especially the 'Urgent' indicator) to preserve their impact. The default system configuration should make both buttons readily available from the application toolbar.

Content

Users should be encouraged to stick to one main subject within each email, rather than using one message to cover a wide range of topics. Otherwise not only does it become impossible to accurately express the nature of the content in the subject heading, but it is also difficult for the recipient to apply appropriate management controls to the email (into which folder should it be stored, how long should it be kept, etc).

Users should also be trained to avoid the growing tendency to use abbreviations and 'text message' language within emails. Such shorthand can easily cause confusion and mis-

interpretation. Likewise users should be made aware of the benefits of using objective, conversational English and avoiding subjective comments or jokes which can be easily misconstrued.

Email Disclaimers

The value of email 'disclaimers' attached to every email sent by the institution and specifying the conditions under which the message has been sent and should be treated is hotly contested. On the one hand their legal status and the level of protection they offer is at best limited (if not non-existent), and yet on the other hand virtually every organisation - including legal firms - seem compelled to include them; suggesting they must have some value.

The Case 'For' Disclaimers

Thanks to the legal concept of 'vicarious liability' the institution is responsible for the actions carried out by its staff - hence the whole reason for institutions to be concerned by how their staff use email in general. However, the institution may also be held liable by a recipient who believes they are communicating with a genuine member of staff even if they are not. A disclaimer can help clarify the legality of an email and the way in which its contents should be interpreted.

The Case 'Against' Disclaimers

Most disclaimers are poorly drafted, inappropriately situated within the message and used indiscriminately - thus removing most, if not all, of their effectiveness.

For example there is little point attaching a disclaimer to the very bottom of your emails (where the vast majority are situated) which states words to the effect of "if you are not the intended recipient of this message please do not read it". Likewise where such text is added to emails sent to JSCMail email lists where the message is then sent indiscriminately to hundreds of recipients.

Poorly drafted disclaimers will not only remove any last remaining vestige of legal rigour, they may also serve to portray a negative image of the institution as either being overly bureaucratic, naive or inept (or all three!).

Institutions are advised to seek their own legal advice regarding the pros and cons of disclaimers and when drafting the text of such a statement if they do choose to use one.

Some useful and entertaining non-legal advice on this topic is also available from the [University of Dundee](#)

Active Use

The potential range of issues emerging out of the active use of email are widespread and complex, including technical issues surrounding online security and legal issues relating to the monitoring of users online activity. Thankfully the focus of this resource is specifically on the information itself, which in this strand means the actual emails which have been created and are now in 'active use'. Inevitably any discussion of the active use phase of the email lifecycle will have to dip into these broader topics because of the impact they will have on the way in which emails are used and managed. However, it should be noted that the focus of the guidance included within this phase of the infoKit unapologetically remains the management of email itself with only superficial and passing reference to these broader topics where specifically relevant.

The contents of this section builds on and augments the information provided in the Information Lifecycle - Active use strand and should be considered in this light. What this section attempts to do is build on the general good practice guidance on information creation covered previously and look specifically at the additional requirements for managing emails.

As such it will be of use to those tasked with managing and maintaining email services within the institution and those with an interest in the management of information and records.

The topics covered within this section include:

- Monitoring email use
- Remote/home use of email
- Outsourcing your email provision
- Email security
- Making best use of your email application

Monitoring Email Use

As in most areas of institutional life it is comparatively easy to draft and approve policies, such as the Email Acceptable Use Policy mentioned in the previous section. However, it can often prove far harder to actually ensure that the policy is being adhered to. It also raises the question of what the institution will do if and when it discovers user activity which is in breach of its policy. Thanks to the concept of vicarious liability outlined in the section of email disclaimers the institution is liable for the actions of its employees. In legal terms having a policy which is generally ignored and widely flouted is unlikely to be considered much of a defence against any claims of culpability.

However, the institution must also ensure that any actions it takes to monitor the email activities of its staff are also legal and conform to all relevant legislation. Otherwise not only will the institution find itself unable to take appropriate measures against any users found breaching the rules, but may even find themselves on the wrong side of the law with action taken against them accordingly. The key pieces of legislation to consider in this area are:

- [The Regulation of Investigatory Powers Act 2000](#)
- [The Human Rights Act 1998](#)
- [The Data Protection Act 1998](#)

The [JISC Legal Information Service](#) contains specific guidance relating to the monitoring of electronic communications as well as more general information about such. These include:

- Interception & Monitoring Law ([webcast](#))
- Interception & Monitoring Law ([transcription](#))
- Interception & Monitoring Law ([FAQ](#))
- [Data Protection Act 1998](#)
- [Monitoring Internet Use](#)

As stated in all of the above sources, these are intended as legal information only and it is advised that institutions seek their own legal advice in relation to specific issues.

Further information is also available from the [Office of the Information Commissioner](#)

Remote/Home Use Of Email

Email use is no longer tied to the desktop and restricted to the office. A host of technologies now make it possible to create and receive messages whilst at another location or in transit between locations. These are all positive developments that have done much to increase the productivity of users; but at the same time it is important that the risks inherent in such flexibility are

recognised and addressed. The institution should seek to ensure that same level of management control is extended to the active use of email where ever and how ever it is being used.

It is important that remote and/or home workers recognise that the emails they work with 'off campus' are subject to exactly the same policy framework as all other institutional emails. This should be communicated to any users affected as part of the terms and conditions of working remotely.

It will prove easier to retain a consistency of approach to email management, regardless of location, if staff email is configured on an IMAP rather than POP basis. Use of IMAP ensures that all messages contained within a user's email account are stored centrally on the institution's servers and are only retrieved when required. A POP-based email service downloads messages for storage on the individual user's machine resulting in a range of potential management problems as indicated in the table below:

Table outlining the management problems associated with POP-based email provision

Issue	Implications
Information loss	Unless copies are also being retained on the server any fault or theft of hardware could result in valuable information being irretrievably lost
Information security	Loss or theft of hardware could result in sensitive or confidential information falling into the hands of 3rd parties. There are countless examples of laptops containing such information being stolen from cars, hotel rooms, conferences etc.
Legal discovery	Emails stored locally may not be located or accessible if required as part of a legal discovery exercise or request for information
Inconsistent retention	Emails stored locally are less likely to be retained or destroyed according to pre-defined business rules
Gaps in the evidential record	Emails stored locally will not be accessible to others and important information may appear to be missing from the information associated with a particular process or transaction.
Preservation	Emails stored locally are less likely to be subject to any institution-wide preservation activity, thus increasing the chance of them becoming inaccessible over time

Those using mobile devices such as Blackberries should ensure that access to the device is password controlled. They should also be encouraged to resist the temptation to adopt a 'text language' approach to creating emails on such devices. Abbreviations and use of slang are open to mis-interpretation and are not appropriate for what may form part of an official business record.

Outsourcing Your Email Provision

Trinity College Dublin hit the headlines earlier this year with the announcement that they are to outsource their entire institutional email service to Google. Other institutions seem set to follow suit and realise the significant cost savings which may go with the outsourcing of your email service.

It is outside of the remit of this resource to offer any judgement on the nature or degree of financial savings that can be realised, or the technical implications which are associated with making such a move. Instead what follows are some aspects to consider prior to embarking on this course of action which may affect the way in which your institution is able to manage the emails it uses.

It is important that the institution realises that although it may be outsourcing the technology and service provision it cannot simply divest itself of responsibility for email management by outsourcing its liabilities to a 3rd party. The concept of vicarious responsibility will still apply and the institution is still liable for the emails created or stored by its users. Recognition of this fact colours many of the remainder of the issues to be considered, revolving as they do around the need to continue to meet these responsibilities even when you are not in day to day control of service provision.

Consideration should therefore be given to the following issues:

- Are you aware of the type and nature of personal data collected by the service provider about your users? Is this in line with your legal responsibilities, is it ethically defensible and has it been communicated to your users?
- Are you aware of who will own the copyright contained within the messages stored by the service provider? Have you considered the implications if copyright is to rest with the service provider?
- Are you aware of and comfortable with the level of back-up and disaster recovery measures being offered for your email?
- Are you aware of how long the emails created or received by your users will be routinely retained by the service provider?
- Are you able to define and enact your own retention actions on the emails stored by the service provider according to the messages content?
- Are you comfortable with the level of preservation measures available and their ability to provide continual access to emails for long periods of time (for example over 50 years)
- Will you be able to extract and move all of the emails your users have created at any point in the future to another service provider (or back in house)?
- How quick and easy will it be for the institution to update or remove a user's system privileges?
- Have you considered how this hosted service will interact with other institutional systems? How easy will it be for users to associate the contents of emails held by the service provider with related information held within the institution? What impact may this have in terms of resource discovery and management?

Careful thought should be given as to whether outsourcing is the right move for the institution if the proposed service provider is unable to provide satisfactory answers to any of the above - regardless of any perceived immediate technical or financial benefits.

Email Security

The question of email security is addressed within this resource from a broadly non-technical perspective and instead focuses on the role of the user in this regard and the role they must play in protecting the security of the emails they create and use.

Perhaps rather strangely one of the key messages that users should be supplied with with regards to email security is that email is inherently insecure. Unless specific measures have been

taken to provide a secure, encrypted system users should be made aware of the limitations of current security provision. Such technical limitations may have a bearing on the institution's acceptable use policy by prohibiting the use of email to transmit sensitive or confidential material due the institution's inability to provide appropriate levels of security for such information.

Passwords & User Behaviour

Users should be provided with guidance as to what makes a good or bad password and encouraged (if not forced) to change them regularly. If no password is required to access a user's email account once they have logged on to their machine they should be encouraged to make use of password controlled screensavers, especially if working in an unsecured area. Password-controlled access should also be enacted on any mobile device used to send or receive email.

Institutions need to be mindful that whilst the majority of their staff are likely to be experienced email users, there may also be a small number who are using it for the first time and who are less aware of the dangers posed by viruses, spam and email 'phishing' scams. Care should be taken to ensure that appropriate guidance and awareness training is provided for such 'novice' users.

Account Maintenance

Institutions should ensure they have well established procedures for terminating access to a user's accounts when they leave the institution. This is particularly important now that virtually all institutions offer a webmail service which would allow the former member of staff to continue to access and use their account even without access to the desktop email application.

This of course raises the question of what should happen to the contents of a user's email account when they leave the institution. This subject will be addressed in the Managing Email Retention section of this resource.

Making Best Use Of Your Email Software

Most email applications contain a significant amount of functionality which can be routinely employed by users to better manage their inbox. By doing so they not only help lessen the burden of trying to keep pace with their email, but by extension they also help reduce the institution's exposure to risk by decreasing the likelihood of inadvertent user error. Unfortunately users are seldom made aware that such functionality is available to them or provided with training in its use.

The following table demonstrates the range of 'inbox management' functionality available within Microsoft Office Outlook 2003. Functions may vary, or not exist within other applications.

Table illustrating email application functionality and its use in email management

Function	Use
Changing the colour of messages addressed solely to the recipient	Makes it easy to see at a glance which messages are addressed solely to you (often an indicator of messages requiring more immediate attention and action).
Adding 'flags' to messages from certain people or containing certain characteristics	Useful for quickly sorting, prioritising and arranging messages.

Turning off the new message notifications	Prevents users from being constantly disrupted and diverted from their work every time a new message is received.
Creating and naming sub-folders to match your main shared filing system	This makes it easier for users to manage their email in tandem with the other information to which it relates. It also makes resource discovery across systems easier.
Create rules to automatically move emails matching certain criteria into the appropriate sub-folder	Acts as a useful default pre-sorting of content. It also helps increase the obvious value of ensuring emails have accurate subject headings.
Ensure emails are removed from your 'Deleted items' folder on application closure	This ensures that emails intended for deletion are removed from the user's application and do not inadvertently remain.
Save replies with the original message	Can be useful for ensuring that both sides of a transaction (i.e. messages both sent and received) are captured and managed as one.
Out of office assistants	An important requirement to ensure compliance with the FOIA. Enacting an out of office alert which includes an alternative contact point will 'stop the clock' of any request received.

The [Managing Information To Make Life Easier: A Guide For Administrators](#) resource provides further practical tips to help users manage their email more effectively.

Semi-Active Use

Email is not only a quick, convenient means of transferring ephemeral information. Emails can be, and often are, formal business records which provide evidence of important transactions. Most of the guidance relevant to the semi-active phase of the lifecycle reflects this need to manage emails as records. Although a consideration throughout all phases it is largely in this semi-active phase, after their initial reason for creation and active use have declined, that the majority of these factors will come to light.

As the active use of the email declines so too often will the interest of the user. This can lead to a management vacuum which in turn leads to inconsistent measures being applied, or worse still no measures at all. It is important that the institution takes action to fill this void from the centre, thus protecting its interests and helping the user to operate effectively.

The contents of this section build on and augment the information provided in the Information Lifecycle - Semi-active use strand and should be considered in this light. What this section attempts to do is build on the general good practice guidance on information management covered previously and look specifically at the additional requirements for managing emails.

As such it will be of use to those tasked with managing and maintaining email services within the institution and those with an interest in the management of information and records.

The topics covered within this section include:

- Identifying emails as records
- Managing emails as records
- Managing email retention
- Managing email retention in context
- Finding emails

Identifying Emails As Records

Given the tremendous volume of emails sent and received by the institution each day it is neither practical nor desirable to manage each and every one as a formal business record. The trick is to be able to identify and capture that small percentage of emails that need managing as records - to separate the wheat from the chaff.

This will depend in part on the institution having formally defined what constitutes a 'record'. Further information on what properties and characteristics define a record are included in the Records Management - What is a Record? Section . The whole records management strand of this resource is relevant to this area in terms of identifying the specific qualities associated with records and the management controls required to preserve them.

It is also important that users are given clear, simple guidance on which of their emails might constitute records and require handling accordingly. This should include both categories and possible examples. For example:

Category	Example
Formal agreements	Approval of contracts, project plans, policies, etc.
Decisions/confirmation of actions	Approval to spend money or to carry out a particular activity
Confirmation of completion	Project sign off, receipt of goods, etc.

Next Steps

It is one thing to equip the user with the ability to identify the records contained within their email, but this is of little consequence if they are not also given the means to act accordingly. For those emails which are identified as being records it is important that they are formally recognised as such and managed in context with the other records to which they relate. This is likely to require the transfer of the email record from the user's inbox to whatever facility is being used to store and manage all other records within the institution. This may be either a shared file server, document/records management system, repository or collaborative technology such as Microsoft Office Share Point. It could even mean printing out the email and managing it as a hard copy record if no suitable electronic facility exists.

It must be made as easy as possible for users to transfer email records to such systems so as not to erect any unnecessary barriers to this process. The email records should be transferred to the appropriate area of the record-keeping system and then managed in a consistent manner to all

other corresponding records. In this way the email record will be managed appropriately according to its content and not based on the fact that it happens to be an email.

Managing Emails As Records

The transfer of email records to the appropriate recordkeeping system as described in the previous section is a critical stage in the process. However, the simple act of transferring the email record is not in itself sufficient to ensure the preservation of their evidential and informational value. Everything possible must be done to ensure the maintenance of the email's record-like properties and characteristics during and after this process. These properties include the following (all of which are explained in more detail within the [Records Management strand](#) of this resource) Authenticity, Completeness, Reliability and Fixity.

Authenticity

In order to demonstrate the authenticity of the email it is important that all sender and recipient information is carried over with the email record - including all parties receiving the email as a carbon copy (CC) or blind carbon copy (BCC). Some legal opinion also asserts that an email can only be considered a legal record if the author has manually typed either their name or initials at the end of the message. Reliance solely on a name which is automatically included as part of an email signature may not be regarded as sufficient in this regard.

Completeness

The completeness of the email as a record can only be assured if all component parts of the email are transferred and retained together as a single record. This includes the text contained within the email itself, the transmission data included within the email 'header' and any attachments originally associated with the message.

Reliability

As with all records it is largely up to the original author to ensure that the contents of the email record are accurate. However it is also important to be confident that nothing has changed within the content of the email record during the process of transfer to the record keeping system. This may be especially relevant if the format of the email is being changed during this process (i.e. from its native Outlook Message Format or HTML into a text file).

Fixity

It is important to ensure and be able to demonstrate that no element of the email has been or can be altered in anyway after being declared as a record. This includes changes to the content, but also to the transmission data and the content of any attachments transferred with the original message. This may be variously achieved by altering the properties of the file to a 'read only' status, or modifying the permissions within the specific area of the record keeping system to prevent further amendment.

Managing Email Retention

"Does your organisation retain all your email forever? Congratulations. You are a disaster waiting to happen." (Amacom, 2003)

The costs and dangers associated with keeping too much information, and the risks of not retaining the right information have already been covered in the [Records Management strand](#) of this resource. The same drivers apply equally to the retention of email and yet as a rule it is an area that if not ignored completely is usually handled inappropriately.

By What Criteria Should Email Retention Be Decided?

The only restraint usually placed on the retention of email is the imposition of pre-set storage quotas on individual user accounts. The intention of such limits is to prevent the unlimited accrual of email but adopting this approach does little to achieve this. When confronted with an 'inbox full' message most users will simply 'archive' a vast chunk of their messages and store them on their desktop as .pst files. In this scenario not only do the emails still remain, but they are now contained within an unmanaged and inaccessible local silo.

Alternatively users will often simply select those emails with the largest attachments that they have no immediate use for and delete those in order to reduce their account size back to a 'legitimate' level for a few days. Both of these represent retention management based either on file format or file size and neither pay due attention to the email's content: the property which should be the key determinant of its retention.

Retention Based On Content

It is one thing to state that email retention should be determined by its content, but quite another to enable this. Firstly it assumes that you have a retention schedule in place which defines the appropriate [retention period for records](#) of various types. Secondly it relies upon each user being able to quickly and easily make the right decision regarding the content of an email and how long it should be retained for - no easy task given the vast number they receive each day.

Separating The Wheat From The Chaff

The process of separating email records from email ephemera as outlined in the previous section has an important part to play in making this task more manageable. One way of doing this is to consider introducing an automatic deletion policy for all emails older than a certain amount of time (perhaps 90 days). After this time (by which any initial informational value is likely to have expired) the email is routinely removed from the user's inbox and permanently deleted. This relieves the user of the need to concern themselves with managing the ephemera - leaving them to concentrate on what they must do with the small proportion of emails which should be managed as records. This policy is not without risks, dependent as it is on the user to identify which emails are records and to categorise them according to their content to ensure their appropriate management. Being forced to choose what emails they must keep as opposed to which they should delete is a subtle, yet profound, change to the culture of email use and the role of the user within it and is not something to be introduced lightly or without due prior training and awareness raising.

Managing Email Retention In Context

What we are trying to achieve in this and the previous section are ways of ensuring that email retention is managed in the same way as the retention of any other type of record. This is why the sections of records retention are so relevant to this topic. At the same time we cannot ignore the fact that the volume and nature of email as a format adds the difficulty of achieving this. Routinely removing ephemera as previously described can be successfully adopted as the first stage of the process. The next step requires the user to transfer their email records to whatever repository is being used to store the other records to which they relate (for example shared file server, document management system etc).

Ideally users would do this as and when such email records are identified. That way the email records they possess become part of the institution's 'official' shared and managed information holdings as quickly as possible. In reality, however, this may prove unworkable where large numbers of email records are being created or received by busy members of staff. In such circumstances an acceptable compromise might be to encourage transfer of all such email records at defined points in the process. These may include official project gateways and review points or at project closure for smaller projects, completion of a tender process or of the entire

contract to which it relates etc. The Semi-active use - Do you know what information is being held and why? section of the Information Lifecycle strand of this resource provides further information about how to identify these points in the lifecycle of information - reflecting as they do the dividing line between active and semi-active use.

By encouraging users to create email folders which mirror those of the main record/document filing system as suggested in Active Use - Making best use of your email application section it should prove easier for the user to quickly and easily identify the correct folder for these emails to be transferred to.

What Happens When A Member Of Staff Leaves?

If the institution has adopted the measures outlined within this resource it is to be hoped that a departing member of staff's email account should only contain a relatively small number of messages relating to current activity. These should be arranged in such a way that it is then a comparatively easy job to transfer them over to the respective folders to which they relate in the main shared file area as part of their hand-over activities.

Unfortunately what institutions will also often find are that the accounts of departing staff contain hundreds if not thousands of random, unmanaged emails relating to a wider range of topics: trivial and important; current and completed. In this scenario the institution has three basic options: to go through and sort them out individually; to keep them all or to destroy them all. Which of these is adopted will depend upon the number of emails in question, the seniority and importance of the member of staff concerned and the degree of risk it is believed retention of the total collection involves. If the institution does decide to retain all messages when an employee leaves it is suggested that a policy is enacted whereby any of their emails then subsequently accessed are transferred into the appropriate 'corporate space' and that after an agreed period of time (3 years?) the remainder of their emails are permanently deleted.

Finding Emails

As we have seen, emails can often contain valuable and important information, they can also act as vital links in the chain of evidence required to justify a course of action or protect the institution's legal interests. Any of this is only possible if all relevant emails can be identified and located when required. The focus during this semi-active phase of the lifecycle is therefore less on ensuring that the individual user can navigate their emails effectively and more on the issues presented by the need to locate emails from across the entire institution in response to an external demand. That said the ability to meet these demands as an institution will largely be dependent on the actions of individual users and the way in which they create, name and manage their messages as described in the creation and active use phases.

The Advantage Of Central Storage

Any form of external request for information held by the institution, be it an FOI or Environmental Information Regulations Request, Subject Access Request under the Data Protection Act or any other type of legal discovery exercise may well cover emails received by staff across the length and breadth of the institution. This is one of the reasons why the use of IMAP over POP as the method of retrieving emails is recommended - see Active use - Remote/home use of email for further details. Central storage of emails at least provides the potential for cross-server analysis and resource discovery using any one of a number of commercial email management or 'archiving' software. Emails stored locally on individual PCs, laptops or external storage media will not be covered and therefore may not be found during any such discovery exercise.

It is important that any such analysis of staff user accounts is conducted in accordance with the law, as outlined in the Active use - Monitoring email use section.

It is more likely that any discovery exercise will relate to a specific topic or event ("I would like to see all information relating to topic X", or "there is a court case pending relating to the patent of

research project Y") rather than just to email specifically. It is for this reason that we suggest managing email alongside all the other information to which it relates. That way all information relating to topic X or Y will be located and easily retrieved from one place.

User Behaviour During A Legal Discovery Exercise

Despite these measures it is inevitable that individual users will hold emails and other information which relate, no matter how tangentially, to the topic under investigation. Any staff who are believed to have played a role in the process or to have received information relating to it should be immediately and explicitly instructed not to delete any emails which relate to the area under investigation. They should then be asked to identify and make available any relevant emails for inspection. The compulsory nature of this instruction, the need to ensure comprehensive disclosure and the necessity of its swift completion should all be communicated to the user (who may otherwise consider it to be of low priority). The relative ease with which staff are able to carry out their role in this process will largely be determined by the degree to which the measures outlined in the creation and active use phases of this resource have been adopted.

Final Outcome

As with all other types of information it is important that any emails worthy of long term or even permanent retention are identified and managed in such a way as to enable continued access to them in the years to come. Conversely it is equally important once the decision has been taken to delete an email that all instances of it have been completely and unequivocally removed. This last phase of the lifecycle focuses on these two possible final outcomes.

The contents of this section build on and augment the information provided in the Information Lifecycle - Final outcome strand and should be considered in this light. What this section attempts to do is build on the general good practice guidance on information management covered previously and look specifically at the additional requirements for managing emails.

As such it will be of use to those tasked with managing and maintaining email services within the institution and those with an interest in the management of information and records.

The topics covered within this section include:

- Archiving & preserving emails
- Deleting emails

Archiving & Preserving Emails

It may seem unlikely that your institution will ever want to permanently preserve an email - after all they are hardly the same as the ancient charters written on parchment, or the vast ledgers and accounting books which may feature in your historical archive. But it is important to remember that years ago those ledgers and accounting books were also seen as bland functional, administrative records of operational rather than historical value. The emails informing staff that the institution has been awarded university status or is to merge with another college are obvious examples of messages which need preserving as part of the historical record. Other examples might be less obvious but are likely to be characterised as emails which answer the what, when, why, who and how questions associated with major developments within the institution. As ever, the secret is not to manage emails based on the fact that they are emails, but according to their content. As such emails of potential historical value should be identified and captured according to whatever policies your institution has in place for identifying its archival records. The [guidance on Archival Appraisal](#) which accompanies the JISC infoNet Records Retention Schedule provides advice in this regard.

Alongside the few 'historic' messages which may require permanent preservation there is also likely to exist another category to be considered: those emails which for operational reasons need to be retained and accessible for a long period of time. It is hard to put a precise number of years against what constitutes a 'long period of time', but when talking about information held in electronic format this could be as little as anything older than five to ten years. Without taking special measures to ensure their continued longevity it is likely that emails older than this will lose some or all of the characteristics required to retain their evidential status as records (see the [records management](#) strand of this resource for further details of these characteristics). Emails relating to building projects, long term contracts, research trials and employment matters amongst others could all fall into this category.

The measures required to preserve such emails and to provide continued access to their content can be complex and will require a mixture of policy, technology and user participation - starting with the need to identify potential candidates for preservation at the earliest possible stage. This will inevitably require the participation of users so training and awareness of such issues as part of general email training is likely to feature as an important first step.

The JISC Digital Curation Centre has produced an excellent, detailed, set of guidelines on the [curation of email](#). It is a comprehensive, yet readable, guide to the subject and is recommended as the source of detailed guidance in this area.

Deleting Emails

The process of deleting and destroying email is of course closely associated with the subject of retention - destruction being the logical outcome when an agreed retention period has come to an end. As such the guidance in this section should be read in association with the sections on email retention.

However, rather than focusing on when an email should be scheduled for destruction the purpose of this section is to explore the issues surrounding the actual destruction process.

Has Your Deleted Email Really Gone?

It is important that the process of deleting emails is comprehensive, complete and irrevocable. After all, there is little point in ensuring the destruction of one copy (perhaps the one held in the sender's sent items folder) if each of the five recipients has retained their own copies. Even if the intention is for the email in question to have been removed the fact that a copy still exists is enough for it to be disclosable under FOI or as part of a legal discovery exercise. The need for such a comprehensive approach to email destruction is one reason why the author of this resource favours the introduction of an automated email deletion process after a relatively short period of time - even with its attendant cultural and procedural problems. However even this will not be sufficient if users are routinely storing their emails 'offline' either individually or collectively as monthly .pst folders to escape the automatic deletion process.

As stated above, email deletion must also be irrevocable. The guidance from the [Information Commissioner's Office](#) is explicit in its assertion that:

"Information located in desktop recycle bins is clearly subject to the FOIA as this continues to be held and is easily accessible. Once deleted from the recycle bin the information will also continue to be held unless the electronic record is completely erased from the computer system."

The issue becomes slightly greyer when it comes to the subject of email stored on back-up servers as the following quote from the same source indicates:

Information in a deleted file or in a back-up, whether a server, disc or tape, may be regarded as being held by a public authority for the purposes of the FOIA depending on the particular circumstances of the individual case. (Our position on this issue has been modified in the light of the Information Tribunal decision in [Mr P Harper v The Information Commissioner EA/2005/0001](#)).

For the avoidance of doubt it is therefore recommended that procedures be put in place to ensure that the contents of back-up tapes and servers are also subject to pre-defined, agreed and documented retention controls. This will help prevent both potentially expensive trawling of vast volumes of data potentially stored in multiple locations and the possible disclosure of messages thought long departed.

Disclaimer

We aim to provide accurate and current information on this website. However, we accept no liability for errors or omissions, or for loss or damage arising from using this information.

The statements made and views expressed in publications are those of the authors and do not represent in any way the views of the Service.

The JISC infoNet Service offers general guidance only on issues relevant to the planning and implementation of information systems. Such guidance does not constitute definitive or legal advice and should not be regarded as a substitute therefor. The JISC infoNet Service does not accept any liability for any loss suffered by persons who consult the Service whether or not such loss is suffered directly or indirectly as a result of reliance placed on guidance given by the Service.

The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and email addresses should be used with caution. We are not responsible for the content of other websites linked to this site.

This material is licensed under the [Creative Commons License](#) - 2007