



Email as Records: Advice to Victorian Government Agencies

This information sheet provides general advice to Victorian government agencies on the management of email as a public record.

Public Record Office Victoria (PROV) has developed a strategy for dealing with public records in electronic form. This strategy (called the Victorian Electronic Records Strategy or VERS) is outlined in *The Victorian Electronic Records Strategy Final Report* and in PROV's *Standard for the Management of Electronic Records* (PROS 99/007). This Advice expands on that given in VERS and provides guidelines to agencies on managing email which constitutes a public record.

The use of email has become increasingly prevalent in the way that the Victorian Government conducts its business. A significant amount of information that may have previously existed in hard copy form now often only exists as part of an email message, in electronic form.

Email systems create electronic records but do not manage them very well. There is a danger that important corporate records may be lost if they are not properly managed.

Email is a record

Public Records are defined by the *Public Records Act* to be "any record made or received by a public officer in the course of his duties"¹. As emails are made or received by public officers as part of the jobs they do in government they are definitely considered to be public records.

Recently the PROV received advice from the Victorian Government Solicitor which supports this statement. In it the Solicitor noted:

it is my opinion that an e-mail made or received by a public officer in the course of their duties, even if it is only stored in electronic form, is a "public record" within the meaning of the PR Act²

Records can be made up of one or more documents. This is often true of emails which may be made up of an email plus attachments. In this case the record would consist of both the email itself and its attachment(s).

¹ s2 *Public Records Act* 1973

² Advice received from Victorian Government Solicitor's Office, 4 January 2002.

Types of Email

Email created or received by most agencies can generally be divided into three different types.

- **Personal email** – email which is of a personal nature and which has no relevance to the business of the agency
- **Ephemeral email** – email which is used to facilitate agency business but which does not need to be retained for business purposes
- **Corporate email** – email which relates to the business of the agency and which must be retained as a record

These three categories are discussed in greater detail below:

Personal Email

Personal email is email which relates to a private or personal matter and has nothing to do with the business of the agency. Examples of personal email includes email dealing with topics such as:

- let's do lunch
- personal/family arrangements
- unsolicited information or jokes not related to staff work responsibilities

If an email incorporates personal and work-related information, then the email is a public record.

Disposal Recommendation: Personal email can be destroyed as soon as staff no longer require the email.

Ephemeral Email

Ephemeral email is email which facilitates agency business but which does not need to be retained for business purposes. Examples of this type of email include:

- Notices of meetings
- Copies of minutes
- Copies of reports or newsletters
- Staff movements
- Advertising material and any other publicly available material
- Internal work-related email received by “carbon copy” (cc) or “blind carbon copy” (bcc).

Disposal Recommendation: Ephemeral email can be destroyed as part of normal administrative practice in keeping with the *Public Records Act*.

Corporate Email

Corporate email forms part of the public record. It is email that documents the business activities of the agency. Examples of emails which form part of the public record include:

- A communication between staff in which a formal approval is recorded
- A direction for an important course of action
- Business correspondence received from outside the agency

Disposal Recommendation: Corporate email must be retained for as long as is determined either by the relevant *Disposal Schedule* or, if the records are not covered by any schedule, by the Keeper of Public Records.

Checklist for Identifying Email Category

	Yes	No
1. Does it relate to work?	<input checked="" type="checkbox"/> Go to 2	<input checked="" type="checkbox"/> Email is personal and can be deleted
2. Am I sending an email to another staff member (or members) which will require action?	<input checked="" type="checkbox"/> Email is a corporate record and should be filed	<input checked="" type="checkbox"/> Go to 3
3. Am I sending an email to another staff member (or members) which authorises a piece of work?	<input checked="" type="checkbox"/> Email is a corporate record and should be filed	<input checked="" type="checkbox"/> Go to 4
4. Does this email, which I have received, relate to business correspondence?	<input checked="" type="checkbox"/> Email is a corporate record and should be filed	<input checked="" type="checkbox"/> Go to 5
5. Am I replying to an external email which is business correspondence?	<input checked="" type="checkbox"/> Email is a corporate record and should be filed	<input checked="" type="checkbox"/> Go to 6
6. Am I sending an email which is business correspondence?	<input checked="" type="checkbox"/> Email is a corporate record and should be filed	<input checked="" type="checkbox"/> The email is ephemeral and can be deleted

Email systems and risk

As stated earlier, email systems do not manage emails very well. This is especially true if you have a system where email is regularly purged when mail boxes become too large or when staff members leave. When important corporate records (such as emails which authorise financial decisions or policy changes) are lost, agencies may face increased legal and social risks. For example, they not be able to justify their own decision making processes because they cannot find supporting documentation. They may be unable to ensure that all staff have access to appropriate information and so decisions may be made which are misinformed or incorrect. These risks can only be managed by assessing the agencies email system and putting in place a strategy (or strategies) to reduce these risks.

There are a number of factors which should be taken into account when determining the appropriate strategy for your agency.

Corporate email should be accessible

Emails which form part of the corporate record should be able to be read by anyone who has sufficient access privileges. That is, authorised staff should be able to read emails which are relevant to their business regardless of which email inbox the email was sent from or to. However, many email systems only allow the recipient or the creator of emails to access those messages. This means that some alternative method for providing access to those corporate emails must be found.

Records should not be altered

It is important that records not be able to be altered (or that alteration only happen in an authorised fashion), otherwise they may not be considered reliable evidence. Many email systems allow users to alter their messages after they have been sent or received. In the event of a dispute about the content of a particular email, the ability to prove that the version of the email being advanced as the record is identical to the version that was sent or received is paramount. Thus, a method must be devised that ensures that emails that are

records cannot be altered after dispatch or receipt, or, at least, that any such alterations cannot be made undetectably.

Records should be classified

An important component of email (and other records) management is classification. That is, emails should be filed so that they are related to other documents (paper or electronic) on the same subject. If this is done, it is possible to build up a complete picture over time of events related to a particular subject or client or project. If this is not done and related emails are scattered across the agency, it is very difficult to guarantee that **all** emails which are relevant have been found.

Corporate email should be readable for the long term

Finally, it is worth noting the problem of technological obsolescence. It is highly likely that email kept in most email systems will be unreadable in as little as 5 years time. This may not be important for some records, which are not required for more than 2 or 3 years, but will be very important for some other records, especially those which are deemed to be important records of the state which must be preserved forever. It is for this reason that PROV developed the Victorian Electronic Records Strategy.

Managing email as a record

The principal responsibilities required by the *Public Records Act* (and other PROV-issued standards and guidelines that support this legislation) relate to the appropriate preservation of public records, by:

- identifying emails that are corporate business records and destroying those that are not;
- managing email generally as part of day to day use; and
- managing the long term requirements for email.

There are several ways that email can be better managed in your organisation. The methods described are not necessarily mutually exclusive and can often be used together.

Print and file

The least technological approach to managing email as a record is to print and file emails on the appropriate corporate files. This means that emails which are records will be available for others to read, they will be located with other relevant records, they will be at a reduced risk of being tampered with and they will be safe from technological obsolescence.

The difficulties of printing and filing email are that it is time consuming and annoying for staff to have to do. Any policy and/or procedures you devise should recognise that this is burdensome to staff and explain the reasoning behind the decision.

It may be that you can incorporate some automated business rules into your email system so that people are not printing and filing copies which have been cc'd to them from an internal source (for example). This will cut the burden on staff if the amount of email they have to print and file is reduced.

Replicate the file classification structure

An alternative approach is to replicate the paper file structure (sometimes called a records plan or classification structure) in your computer network directories and then make sure that electronic objects (emails, databases, word documents, web pages, etc) are stored in the appropriate directory even if a paper copy is not stored on the paper file. This means that emails which are records will be available for others to read and will be located with other relevant records.

There are some problems with this approach. Some email systems do not allow for the easy storage of email outside the email system (eg Lotus Notes). Unless tight controls

are set on the network directories, emails (and any other objects stored there) may still be subject to tampering. This method also does not ensure against technological obsolescence.

This method should be seen as an interim solution only to be instituted in the short term (3 years maximum) until a better solution can be put in place (like a VERS compliant electronic records management system).

Corporate email boxes

Corporate mail boxes can be set up relating to subjects, clients or projects. All relevant corporate email can be forwarded (if received) or cc'd (if sent) to the appropriate mail box with a code in the subject line. The mail box is divided into a number of folders (relating to individual subject or client or project files). An automated program can be written to sort the email into the appropriate folders based on the code in the subject line or this can be done manually by a file clerk. Multiple users should have read-only access to these mailboxes so that the appropriate people can access relevant corporate email.

Here is an example:

A staff member is working on a specific policy initiative in the Dog Licencing Branch of the Victorian government. The initiative has a number of files including 'Marketing and Promotion (code 23)', 'Administration (code 13)' and 'Working Group (code 16)'. Here is an email written by the staff member which relates to the administration of the project.

To: Jane.Bloggs@licence.dogs.vic.gov.au CC: bluecollars@ licence.dogs.vic.gov.au From: Joe.Bloe@ licence.dogs.vic.gov.au Subject: 13: Report on progress Body: Here is a report on the progress of the Blue Collars For All White Dogs project. Attachment: Report.doc

Note the CC address. When this email is sent a copy is sent to the bluecollars@licence.dogs.vic.gov.au mail box. When it arrives a software program looks at the subject line and notes that it has the code 13: in it. It files the email in a folder in the mail box called Blue Collars-Administration (99/13). All members of the initiative team have read-only access to this mail box so they are able to view information on the file. The folder name is related to a paper folder in the Departmental filing system so that team members can also access any paper documents related to the same subject. The folder name is also reflected in the team's network directory structure so that any other electronic documents which relate to that subject can also be viewed.

This solution is a little clumsy because it does not consolidate all the information into one area so users have to search in 3 places (email system, network directory, paper file) in order to find all related material. However, it does get around the problem of printing and filing if you would prefer to keep electronic records in electronic form. The benefits of this solution are that

- it allows access to email by authorised persons,
- it prevents tampering with email and
- it ensures that emails are classified in a similar manner to other corporate records.

It does not ensure that email will be readable for the longer term.

Again, this method should be seen as an interim solution only to be instituted in the short term (3 years maximum) until a better solution can be put in place (like a VERS compliant electronic records management system).

Electronic Records Management Systems

An Electronic Records Management System (ERMS) allows users to file electronic documents (including email) on the same folder (a 'virtual' file). These systems can also be set up to classify, file and manage records. The benefits of such a system are that email (and other electronic records) can be made accessible to others in the organisation in a controlled fashion (through the use of access control lists), email can be classified along with other corporate electronic records and email can be safeguarded from tampering. ERMS also provide other useful functions, like the ability to free text search on email.

Much of this functionality can also be derived from an Electronic Document Management System (EDMS) but you should check to see that this is the case when purchasing or implementing an EDMS.

This solution should also be seen as an interim solution, albeit one which has a longer lifespan than corporate email boxes or replicating the file structure. Agencies which are using or considering the use of ERMS should have in place a plan to become VERS compliant over the next 5-7 years.

More detailed advice on the use of an ERMS and EDMS within a VERS compliant framework can be obtained from the VERS team and from perusal of the approach taken by the Department of Infrastructure in their VERS compliance project.

Legal admissibility of email

The legal admissibility of emails (however they are managed) is not clear. Emails have been used as evidence in court cases but usually the veracity of the email evidence has not been challenged by any parties to the case. Thus, they have merely been documentary supports to oral evidence, rather than substantive evidence in their own right.

Emails are more likely to be acceptable to a court where you can show that the management of email in your agency has occurred in a systematic and comprehensive way. Thus if your agency can demonstrate that it has instituted an email management policy and procedures which are followed regularly by the majority of staff, a court is more likely to accept any emails you produce as evidence as being accurate and trustworthy.

Further Reading

- *Standard for the Management of Electronic Records (PROS 99/007)*, available at www.prov.vic.gov.au/gservice/standard/pros9907.htm
- *Victorian Electronic Records Strategy Final Report*, available at www.prov.vic.gov.au/vers/final.htm
- *Electronic Recordkeeping: Advice to Victorian Government Agencies*, December 2000, available at www.prov.vic.gov.au/publIns/PROVRMadvice1.pdf
- *Scanning or Imaging of Records: Advice to Victorian Government Agencies*, June 2001, available at www.prov.vic.gov.au/publIns/PROVRMadvice2.pdf
- VERS Online Toolkit, available at www.prov.vic.gov.au/vers/toolkit/home.htm

Ross Gibbs

Ross Gibbs

Director & Keeper of Public Records

January 2002