**Email Good Practice Guidelines**

**Information Governance Guidance**

##

## Comments and Suggestions

We welcome comments and suggestions from readers to info@adoptionwest.co.uk. They will help us to improve this document in later editions.

Table of Contents

[Comments and Suggestions 2](#_Toc12720)

[1 Introduction 2](#_Toc12721)

[2 Scope 3](#_Toc12722)

[3 Guidance 3](#_Toc12723)

[3.1 Is email the correct tool? 3](#_Toc12724)

[3.2 What sort of information will you be sending? 4](#_Toc12725)

[3.3 Writing an email and sending 4](#_Toc12726)

[3.4 Replying to emails, reply all and automatic replies 6](#_Toc12727)

[3.5 Response time expectations 6](#_Toc12728)

[3.6 Inbox Management 6](#_Toc12729)

[3.7 Housekeeping 7](#_Toc12730)

[4 Important reminder 8](#_Toc12731)

[Appendix 1 9](#_Toc12732)

[Encrypted Emails 9](#_Toc12733)

[Appendix 2 9](#_Toc12738)

[How to select the right recipients 9](#_Toc12739)

[Managing the Auto-Complete List name suggestions 9](#_Toc12740)

[Selecting recipients from address books 10](#_Toc12741)

# Introduction

The importance of good information governance is highlighted by the Information Commissioner’s Office (ICO) who has and do impose significant financial penalties for breaches by organisations who they felt had not taken reasonable steps to safeguard their information. The ICO defines reasonable steps as:

* having clearly defined information governance roles and responsibilities
* having information governance policies, procedures, and training and awareness programmes
* undertaking information risk assessments
* compliance with good practice such as ISO27001 Information Security Management Standard

Comprehensive information, including latest policies and guidance for our organisation’s Information Governance framework can be found at http://intranet/ig or looking up Information Governance in the intranet A-Z.

Within our Information Governance framework this guidance is designed to enable all employees and members to use email systems responsibly and ensure the organisation complies with Information Governance requirements and our legal obligations as a Data Controller.

The Management Team maintains an oversight of Information Governance across the organisation. The group ensures that the relevant strategies, policies, procedures, guidance, training and controls are in place to enable the organisation to fully comply with the Information Governance requirements and fully respect at all times the information we hold.

# Scope

The organisation’s email systems provide a set of tools to help you manage email messages, calendar, contacts, and tasks, including encrypted email when sharing personal and sensitive information with other parties. As such, it’s at the centre of not only our communications but also enabling effective time-management. Email can provide an invaluable means of communication, but our emails need to be accurate, clear and concise if we want them to be effective. These guidelines outline email best practice for the organisation.

Please note your work email address should not be used for your personal use. This includes not using your work email address for any financial transactions, including online banking or shopping, and registering with non-work related websites. Also never use personal email accounts (such as Gmail, Yahoo Mail or Hotmail) to transfer work data or carry out business.

More details of best practice and ‘how to’ guides for Outlook can be found [here.](https://support.office.com/search/results?query=best+practices+for+outlook)

# Guidance

## Is email the correct tool?

Before drafting an email, pause and consider if it is the most appropriate communication method. Face-to-face or a quick telephone call may be more effective, particularly if the topic is sensitive, confidential or very urgent. Should the communication be more formal, e.g. a letter on headed note paper and signed by the sender. This may then be scanned and attached to an email.

## What sort of information will you be sending?

If you are dealing with ‘personal’ or ‘sensitive’ data and you are sending it to external parties you must:

* Establish that you are permitted to share the information – if in any doubt please check with you line manager.
* Additionally, when responding to a Freedom of Information (FOI) request, always consider the content of your response and whether you would be happy with its disclosure if it were information about you.
* Use an encrypted email system such as GCSX, Secure Email (IronPort) or Criminal Justice Secure eMail (CJSM). Please Note: our standard email system, Outlook, is **not** secure when communicating outside the network. However, as our internal network is secure, emails to colleagues within the organisation (i.e. when they are using a @adoptionwest.co.uk address) are secure.
* For more information regarding set up and use of encrypted email please see Appendix 1 and future guidance shared by managers.

## Writing an email and sending

**Action:** Consider what action you would like the recipient to take when they receive the message and make this clear (if you don’t know neither will they).

**Subject line**: Treat this as the label on the tin. Include (concisely) as much information as possible about what the recipient is required to do, including for example, dates, deadlines, times and locations.

**Email length:** Avoid lengthy emails as the message or action can become lost or confused. If you are communicating complex information then consider using an attachment or link to a document (be mindful that such a link will only work if the recipient also has access to the drive or location where the document resides). Avoid replying with email history unless it is necessary. Indeed as email recipients change the inclusion of the previous threads could result in an information breach.

**Attachments:** Avoid sending large attachments and if the attachments contain documents of a sensitive nature always make sure the email is sent securely or the documents are fully redactedto remove the sensitive data. One alternative is to use a shared folder, SharePoint or an online document management system - subject to availability. For more information contact your manager.

**Email signatures:** All emails (including replies and forwards) should include an email signature which tells recipients who you are, what your role is, confirm the organisation you work for and give an alternative way to contact you. Including a link to our website is also helpful. If you represent the organisation in different roles please ensure you use the appropriate signature.

This is a good example of the standard:

**Ada West**

**Adoption Social Worker**

**Adoption West**

Phone: 07777 777777

Floor 2, Old County Hall, Bythesea Road, Trowbridge, Wiltshire, BA14 8JN

ada.west@adoptionwest.co.uk



Find out more at [www.adoptionwest.co.uk](http://www.adoptionwest.co.uk/)

**Quality check: Always** re-read your emails before sending to check that the correct recipients have been included, the message is clear, that attachments have been inserted and spelling has been checked.

**Recipients:** Firstly,make sure you are sending it to the correct recipients. Consider the recipients of your email and be clear what, if anything you want them to do. It is recommend that ‘auto complete' is turned off as this reduces the risk of e-mails containing personal and sensitive information being sent to the wrong person.

* The “To” field should only be used for recipients who you are asking to take action.
* The “cc” field is for recipients who need to see the information. Think carefully about who you need to communicate with and limit the ‘ccs’ to this group only.
* The “bcc” field should be used if you do not wish to share an email addresses with other recipients.

Appendix 2 provides guidance on selecting the correct recipient to avoid a message being sent to someone else in error.

If you are sending to a group which contains personal email addresses then it is recommended that the group is addressed via the “bcc” option. For example the panel members are often emailed as a group to let them know of any changes / requests. However as they are all their private email addresses (they don’t have @adoptionwest.co.uk), they should be addressed via the “bcc” option so that they don’t get to see everyone’s personal email addresses john.smith@hotmail.com etc.

**Final check before sending:** It is essential, particularly when dealing with personal or sensitive information, that the recipients are double checked to be correct. Be particularly aware of the risk of selecting the wrong contact where similar names and email addresses are concerned. Sending personal or sensitive data to the wrong people will result in a serious data breach and may result in a heavy fine for the organisation and disciplinary action being taken against the individual(s) concerned. So if in doubt please check and check again. ‘Hovering’ or double click on recipient names will reveal the full email address that will be used when the email is sent. For particularly sensitive cases the second check should be made by a colleague before sending the email.

## Replying to emails, reply all and automatic replies

**Replying to emails:** It should be considered rude and unprofessional to ignore an email, if it has been sent directly to you. If it’s not relevant or you can’t deal with the email don’t ignore it, it takes little time to respond enabling the sender to seek an alternative route. Sometimes we have to politely say no. All the considerations listed in 2. above should also be considered in your response, always keep it clear, concise and polite. Double check that you have addressed all the points/questions that were raised, as this reduces the need for further emails seeking clarification.

**Reply all:** “Reply all” creates large numbers of emails which are often irrelevant. Before using the “reply all” consider if all the recipients need to know or take some action. Also consider whether they should have access to all of the information contained in the message thread, particularly where external partners and or personal/sensitive data is involved.

**Automatic replies:** When you are away from the office for a full day or longer, your “out of office” should be enabled to provide an automatic response to emails received when you are away. It should contain the date you will return to work and an alternative contact or confirmation that the received item will not be dealt with until your return. Also be aware that your out of office email could potentially be seen by anyone who emails you, so do not include any sensitive information and consider whether alternative contact numbers/addresses are appropriate or not.

## Response time expectations

The use of mobile phones and electronic tablets has led to people expecting a very fast response to emails, even at evenings and weekends. During the working week it is not reasonable to expect a response in less than 24 hours. It is certainly not reasonable to expect a response in the evenings and at weekends. If a response is required in minutes or hours, then email is probably not the most effective communication tool.

## Inbox Management

**Frequency of checking emails**: Checking emails too frequently during the working day, out of working hours and during leave can lead to stress. Ideally check your emails 3-4 times on a working day. This will allow you to focus on specific tasks without constant interruption.

**Email preview**: The email preview bubble can often cause a distraction and it is advisable to turn this off or reduce it to a minimum.

**Organising email:** Avoid letting unread emails build up in your inbox. Action your emails by using the Four Ds:

* **D**elete immediately if it’s not important
* **D**o if a response can be made quickly, say between 2 and 5 minutes
* **D**elegate emails appropriately by forwarding to a more relevant colleague or team, letting the sender know who it has been forwarded to
* **D**efer emails that are going to require more of your time in order to respond. Perhaps include in a ‘to do’ list or even plan a meeting to resolve

## Housekeeping

Firstly, the email system should be seen as a communications tool, NOT a filing system for the work we do. All the important communications and attached documents must be moved, attached (by appropriate means) to the supporting business application, e.g. Shared drive or case management system. Anything else should be considered as transient.

Once emails have been actioned and the thread has come to a logical end, the emails should preferably be deleted. Similarly the ‘deleted’ folder should be reviewed and cleared down regularly, ideally weekly or monthly. Any other emails that you must retain should be moved to an appropriate folder and kept there for a reasonable time while the work is active, all others must be deleted. Users are responsible for managing their own email accounts and the folders within them, including the content you keep and delete.

Contact address lists must also be regularly maintained, so please make sure email addresses of clients that are no longer in use are deleted. Please refer to appendix 2 for more information.

The annual data protection training conveys to all employees that they each have a responsibility to handle the data they use according to legislation, standards and best practice. Data held within email accounts is no different. Indeed, as emails sent from Outlook to a recipient outside the network are not secure every email represents a significant risk as it could easily be incorrectly sent/forwarded to an external entity and create a data breach.

PLEASE THINK BEFORE YOU SEND –

EVERY EMAIL IS A POTENTIAL DATA BREACH

# Important reminder

Failure to follow these guidelines will be fully investigated internally and may result in a serious incident requiring investigation (SIRI) being reported to the Information Commissioners Office (ICO) or via the NHS information governance toolkit. For the organisation this could mean reputational damage and/or fines of up to £500,000. In the future, that amount could be increased. For the individual involved, it could result in disciplinary action being taken which could lead to dismissal. For more information please refer to the Employee Code of Conduct[.](http://intranet/content/CEandCR/Sections/MyHR/CodeofConduct/CodeofConductHomePage.htm)

**Please refer to relevant policies and guidance for further information about the Data Protection Act and general Information Governance best practice.**

# Appendix 1

## Encrypted Emails

Encrypted emails are generally only required if the email and/or its attachment(s) contain personal and sensitive data. You may be familiar with solutions for the provision of encrypted email such as Egress and Securemail (also referred to as Ironport or Cisco Secure Mail). Encryption functionality is also included within Outlook in Microsoft 365.

The use of Outlook within the organisation’s network is also secure, so you can send personal and sensitive information to colleagues within the organisation securely via Outlook. So an email sent from a @adoptionwest.co.uk address to a @adoptionwest.co.uk address is secure. However, if the email leaves the network it is no longer secure; so take care when forwarding messages onto colleagues in other organisations. Think and check before you send.

If you are sending personal and sensitive information outside of the organisation via email then you need to use encrypted email. Recipients of a secure e-mail will typically need to register on a website in order to unencrypt messages. Messages received from recipients or instigated by external third parties using an encrypted email system may be received directly into your Outlook Inbox or require you to create a web account.

# Appendix 2

## How to select the right recipients

If you have communicated with the person before, the quickest way to obtain a recipients email address is to simply start typing their name/email address against the ‘To…’ box. The auto complete list will then display all the addresses you have used recently starting with the characters you have entered.

The problem with this is that all the email addresses are similar, well certainly the first part of them, and it’s relatively easy to select the wrong one, sometimes without even realising!

When dealing with personal and sensitive information the use of the auto-complete list carries a very significant risk of sending the information to the wrong person and causing a data breach.

Therefore, this guide recommends that the list is turned off and you enter the addresses manually. However, it is possible to manage your list to reduce the risks.

## Managing the Auto-Complete List name suggestions

**Turn off the Auto-Complete list**

By default, this feature is turned on in Outlook. **To turn on or off Auto-Complete List name suggestions**, do the following:

Click the **File** tab.

Click **Options**.

Click **Mail**.

Under **Send messages**, select or clear the **Use Auto-Complete List to suggest names when typing in the To, Cc and Bcc lines** check box.

**Delete a name from the Auto-Complete list**

There might be entries that you want to remove, such as entries that are no longer current or accurate. To remove unwanted names, do the following:

Select the unwanted name or email address by using the UP ARROW or DOWN ARROW key. Click or press DELETE.

To **remove all names** from your Auto-Complete list, do the following:

Click the **File** tab.

Click **Options**.

Click **Mail**.

Under **Send messages**, click **Empty Auto-Complete List**.

## Selecting recipients from address books

The best way to select recipients is by clicking on the ‘To…’ box to open the ‘Select Names window.

Under ‘Address book’ you can then select the appropriate ‘Contacts list’.

You can, for example, select ‘All Users’ in the ‘Global Address book’ to reduce the likelihood of incorrectly selecting a name of a colleague due to it being the same as an internal staff member.

You can also set up key external contacts in other address books so that you have to deliberately select them, which will reduce the risk of selecting the wrong recipient and incurring a serious data breach. Similarly make sure these lists are up-to-date by always deleting old contacts that you no longer need to contact.