Records management guidance:

Managing your emails

The Freedom of Information Act applies to all information that you receive and create as part of your employment with the University and the Data Protection Act applies to all such information that contains personal data. This includes emails: these are electronic University records and need managing, just like the other records the University creates.

Managing your work emails will help:

- you ensure that you can find what you want when you need it,
- your colleagues to find important information even if you are not in the office,
- your department to save server space and make better use of resources,
- the University to comply with the Data Protection Act and the Freedom of Information Act,
- the University to ensure that your emails carry weight in court (as emails may be requested as evidence as part of legal proceedings).

The University's Records Management Policy states that all University staff who create, receive and use records (including emails) have records management responsibilities. These can be summarised as a responsibility:

- to create appropriate email records;
- to capture important emails in your School's or Service's record keeping system(s);
- to send emails securely;
- to destroy those emails that are no longer needed, and
- to manage emails during absence.

This guidance aims to assist staff to meet these responsibilities with regard to email. It should be read in conjunction with the Records Management Policy, Data Protection Policy, Computing Regulations and other relevant University policies.

Create appropriate records: sending emails

- Think about what information you are communicating before you start (a telephone call or visit in person might be more appropriate).
- Consider whether the email is:
    - for information only?
    - a request for action?
    - a request for information?
    - a response to a request?
- Indicate the emails purpose by entering a short, clear and relevant description in the subject field. The reader should be able to determine what your message is about before opening it, as this will help them to prioritise their time.
- Make it easy to respond to your message by clearly identifying (e.g. by numbering) your questions/requests.
- Avoid mixing personal and University matters in one email. This will mean that you will not have to spend time blanking out irrelevant or personal information if we receive an information governance related request for that email.
- If you are sending your message to a long list of people, or to external individuals (ie non-University of Huddersfield employees) that do not already know each other's email addresses, use a distribution list so that the full email addresses of all the recipients are

not included in the message. Sharing email addresses without the individual’s permission breaches the Data Protection Act.

- You must not disclose information about another person outside the University without safeguards, such as encryption.
- You may only disclose information about another person within the University for legitimate work purposes.
- Your email message may be disclosed in response to an information request under the Freedom of Information Act, the Data Protection Act or as part of a court case. In view of this, take care what you write. Avoid using email to let off steam, including copying the email to a large number of people.
- If you are not acting in your capacity as a member of University staff, please make this clear.
- If your email is about an identifiable living person, the Data Protection Act requires the University to ensure that the information we hold is relevant, accurate but not excessive. So:
    - do not include irrelevant information
    - clearly differentiate between matters of fact, and opinion
    - do not express opinions that you are not prepared to defend or cannot substantiate
    - do not express opinions in areas where you are not qualified
    - always be sure of the facts
    - do not write in anger or in haste
    - always speak respectfully of the person, even when expressing negative information.
- Avoid attaching documents to emails, if a hyperlink to the document can be used, as hyperlinks provide securer access and ensures a common version is being accessed.

Create appropriate records: replying to emails

The guidance on sending emails above also applies, but particular issues to note when replying are:

- You must not disclose information about another person outside the University without safeguards, such as encryption.
- You can only disclose information about an identifiable individual with the individual’s consent.
- You may only disclose information about another person within the University for legitimate work purposes.
- Include the original text in your reply to an email, as this ensures that you have a complete record.
- If you are involved in an email discussion, try to prevent the discussion from drifting off topic. If a new subject is being introduced, start a new email. This will make your email easier to manage, and will mean that you will not have to spend time blanking out irrelevant or personal information if we receive an information governance related request for that email.
- Using “reply all” will send your reply to everyone that received the original email. Before using this option, consider whether everyone included in the original email really needs to see your response.

Capture important emails

- Do not retain emails in your sent items folder – this means they are generally inaccessible to others that might need them, and can make it difficult to retrieve information once the folder becomes too large.
- When dealing with long email strings, provided that the string has not been edited and all previous emails are included, it is sufficient to keep the last email in the string and destroy the earlier ones.
- As well as the text of the email, it is important to keep the associated metadata about the email, such as to, from, date, time, and subject. This is necessary to understand the email and can affect the credibility a court will give to email evidence.
- Consider saving emails to shared folders in Outlook or on the SAN if others need to access the information.
- Where possible, transfer the information from email to the business application that is intended for the storage of that data.
- If you save an email with an attachment outside your mailbox, you should ensure the title associates the items eg. PlanningRound2015-10-27” and the attachment, “PlanningRound2015-10-27Attachment”.
- If you are a user of Wisdom, emails which relate to students should be saved to the student’s file. Often these become relevant to the consideration of complaints, appeals and disciplinary proceedings. The Outlook plug-in tool means that you can save an email direct to Wisdom from your mailbox. Please contact IT Support (it.support@hud.ac.uk) if you need any assistance.

Sending emails securely

- One of the main causes of data protection breaches notified to the Information Commissioner’s Office relates to errors made when sending emails containing personal data, including emails sent to the wrong recipients or containing the wrong data.
- Using email to send personal data should be avoided whenever possible due to the limited protection offered and the inability to retract an email once it has been sent outside of the University.
    - To share sensitive information including personal data inside the University it is more secure to give individuals access to the data at source i.e. give temporary or permanent access to the specific data within the system with their own named account to log in with.
    - Where system access is not possible or where personal data is being shared outside of the University, the use of OneDrive provides security through access rights management (view/amend) as well as the ability to revoke access to the information once it is no longer required by the recipient.
        - For help on using OneDrive to securely share personal data please contact IT Support (it.support@hud.ac.uk).
    - If the information you want to share is held in Wisdom, you can share it with people who cannot usually access that area (internal or external) by using the Halo service. (The document must be marked ‘public’; if it is not, consider that it may not be appropriate to share in this case.)
- Where circumstances dictate email is the only means available to send personal information, ensure the recipient you have entered is correct – remember there is no

way to retract the email once it is sent and loss of personal information would become a notifiable breach which could impact the University. Encrypting an attachment with a password and sharing the password over the phone adds an extra layer of protection.
- Don't include long email strings when replying to or forwarding emails where the strings contain information that does not need to be sent. Take extra care when using the "reply all" function.
- When you start to type in the name of the recipient, your email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - e.g. "Dave" - the auto-complete function may bring up several "Daves". Check and double-check the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure that all of those people really need to see the information in the email before you send it.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

Delete emails which are no longer needed

- If an information governance related request for information has been made, it will be a personal criminal offence to delete email(s) relevant to the request in order to prevent disclosure.
- Requests for information do not have to specify the "Data Protection" or "Freedom of Information Act" to be valid requests, nor do they need to be received through "official" channels, such as the University's Freedom of Information inbox, or using the Subject Access Request form.
- It is not possible to set a standard retention period for all emails because email is used to communicate about such a wide range of things, ranging from the instantly disposable (e.g. canvassing possible meeting dates) to the highly significant (e.g. a decision to commit the University to a significant amount of expenditure).
  The retention period of email is determined by the importance of its contents as with any other record. Therefore, retention decisions have to be taken on a case-by-case basis at the time of receiving or sending email.
  The University's retention & disposal schedule should be used.
  If the email is about an important issue, you should save it to Wisdom, SharePoint, a shared drive or other similar facility so that your colleagues are able to access it easily even if you are away from the office.
- Many emails do not need to be kept beyond the timeframe of the task to which they refer. A simple way to deal with this is to review your sent items at the end of each day and delete those that don't need to be retained. You could also move them to a temporary folder named after the task and then to delete the folder and its contents when the task is complete.
- Delete ephemeral or out-of-date emails as soon as they are no longer required. The most efficient ways of doing this include:

- sorting by date and deleting all those over a certain age;
- sorting by addressee/sender and deleting all those sent to or received from certain individuals;
- sorting by subject and deleting those relating to completed business;
- sorting by size and deleting large emails that are no longer required.

- Opening and deleting individual emails should be avoided as it is time consuming and unlikely to be cost effective.
- When dealing with long email strings, provided that the string has not been edited and all previous emails are included, it is sufficient to keep the last email in the string and destroy the earlier ones.
- Make sure that emails you meant to delete are actually deleted by emptying the deleted items folder.

- If you are the line manager of a member of staff who is leaving, please refer to the Checklist for managing information when staff are due to leave. You should confirm that they have saved important emails to a shared area where they will remain accessible to everyone still employed by the University that needs them. On their last day, the member of staff should either set an out of office message that gives details of a new contact point or arrange to forward all their emails to another member of staff. Within a few weeks of the member of staff's departure, their email account will be deleted from the system.

Manage emails during absence

- Use shared mailboxes and email addresses as far as possible and where appropriate.
- Set an out-of-office message providing an alternative contact point for the time you are absent.
- If you are a line manager and a member of staff is unexpectedly away from the office (e.g. on long-term sick leave), a Dean or Director may authorise access to the member of staff's mailbox and network drive in accordance with the Conduct (Monitoring of Email and Internet use) Policy. Once outstanding mail has been dealt with, an out of office message should be set with alternative contact details.