Guidelines for Reviewing Information on Shared and Personal Drives

Information created and managed by staff, whilst in employment at the University of Huddersfield, are the University's property. Staff are responsible for this information, from its initial creation or receipt, through to its destruction or transfer to the University Archives. Information includes records, documents and data and may be stored in electronic or paper format. This guidance specifically focuses on the information stored on computer drives and in filing cabinets, but its principles can be applied to information stored on databases.

Please note this guidance is for general use. You should also refer to specific guidance, such as that relating to research data, if appropriate.

Why should we review our information?

Currently, the University is experiencing data sharing and retrieval issues, due to the unnecessary retention and illogical filing of its information. This has resulted in shared and personal drives being overrun with redundant records and documents, making current and/or useful information difficult to find. Also information on databases and paper documents in filing systems may contain inaccurate and redundant information. This slows down productivity, increases server/storage costs and takes up vital office space. It also puts the University at risk of breaching legislation, such as that relating to personal data, as we are not fully in control of the information we hold.

To resolve this situation, we need to initially organise and tidy our information to gain intellectual control over what we are creating and managing. Once we have separated useful information from redundant, we will be able to review, devise and implement more 'user-friendly' filing systems, especially within our shared drives, which will improve data sharing and management. This will also enable us to understand what information needs to be shared and in what instances access should be restricted. The University Retention and Disposal Schedule, which has been developed to meet both legislative and business needs, should also be applied to information to ensure it is retained for the correct amount of time and then disposed of. This will ensure that drives remain uncluttered and organised, and that information is easy to find and manage.

The Reviewing Process

You will need to assess **ALL** of the information that you are responsible for and make decisions on what actions should be taken.

N.B. Please contact the Archivist and Records Manager, Amy-Jo Cameron-Williams, if you need any guidance or assistance. Email a.cameron-williams@hud.ac.uk or telephone ext. 3168.

As explained above, information includes records, documents and data.

Amy-Jo Cameron-Williams
University Archivist and Records Manager

March 2018

A **record** can be defined as 'any document or data that form recorded evidence of a business activity.'

A **document** can be defined as 'a piece of written, printed, or electronic matter that provides information or evidence.'

Data can be defined as 'facts and statistics collected together for reference or analysis.'

1. Required Actions

When assessing information and its uses, you will need to decide whether it should be:

- Kept
- Destroyed

To help you assess your information, it is helpful to view records, documents and data as living organisms, whose characteristics change during the different stages of their lifecycle.

Stage 1: Current information: is that which is required daily or regularly for business activities.

Required action: ***Keep***

Stage 2: Semi-current information: is that which is not used regularly, but required for legislative purposes, evidence or reference.

Required actions: ***Keep***

Stage 3: Non-current information or redundant information: is that which is no longer required for business or evidential/reference purposes.

Required actions: ***Destroy***

2. Storage areas to be reviewed

Your information could be held across several storage areas, so please make sure that you check them all. Storage areas include:

<u>Electronic</u>

- Departmental shared drives
- Unishare
- Email
- Legacy/inherited drives
- Other shared drives
- K drives (personal drives)
- My Documents
- Desktops
- USBs

Amy-Jo Cameron-Williams
University Archivist and Records Manager

March 2018

Paper
- Filing cabinets
- Desks and drawers
- Shelves

Only official systems, such as shared drives, Wisdom, Unishare and K drives, are legitimate areas to store electronic information.

Private systems (K drives/My Documents/desktops/USBs)
- K drives are the only legitimate private area to store information. If possible, information **should not** be stored in any other areas (i.e. desktops, My Documents, USBs.) Storing information in these areas places data at risk of loss and hinders data sharing, and therefore business productivity.

- If you do use your own device to store information then you must abide by the University's Using Your Own Device Policy.

- Please assess **all** information within these storage areas (i.e. desktops, My docs, USBs, PC drives).

    - Move current and semi-current information into appropriate official systems.
    - Password protect confidential information on a shared system
    - Move personal or draft work into your K drives

- K drives should only be used for drafting documents or storing personal/confidential information. All other information should be placed within official shared systems to aid data-sharing. If confidential information needs to be shared with others, it is recommended that it is placed in a shared system and password protected.
  IT Support (it.support@hud.ac.uk, ext. 3737) can advise on how to password protect documents.

3. Tidying Advice

A. Delete/destroy duplicate records

All electronic and paper duplicate records should be deleted/destroyed. Examples of duplicate documents include:

- Electronic duplicates or photocopies of records held by other departments, such as:
    - Invoices held by Finance/in Agresso
    - Meeting agenda papers and minutes.

  Only original records should be kept and these should be managed by those responsible for the record.

Amy-Jo Cameron-Williams
University Archivist and Records Manager

March 2018

N.B. There may be one or two exceptions to this rule: for example, financial records that are needed close to hand for reference. Also some financial records may not be held by Finance, and line managers are required to hold a copy of some HR records.

- Paper printouts of electronic records, unless they are contractual paper records with ink signatures, as these should be retained.

B. Rename misleading/miscellaneous folders

- Please ensure that folder names are self-explanatory and not misleading. Please refrain from using words like 'general' or 'miscellaneous'. Vague titles greatly hinder information retrieval. If a folder has a misleading title, please rename it to reflect its contents. Please follow our Advice on naming your files.

C. 'If in doubt, don't throw it out!'

If there are any records that you are unsure of deleting/destroying, because they may be needed for legal purposes, please contact Amy-Jo or consult the University's Retention and Disposal Schedule.

- Seek advice on appraising inherited records/drives/filing cabinets
  Please seek advice from colleagues or get in touch with Amy-Jo if there are any documents/records on inherited drives/filing cabinets that you are unsure of.

D. Legislative issues to consider

- Data Protection
  The Data Protection Act (1998) and the General Data Protection Regulations (from May 2018) ensure that data relating to living individuals is managed appropriately. This means that you need to pay close attention to records that include personal data. Amongst other things, the Data Protection legislation prohibits; the retention of personal data for longer than necessary; the unauthorised access of personal data; the holding of inaccurate data; and holding data without the data subject's permission. We all have a shared responsibility to ensure personal data is managed appropriately.

  For further information, please see the University's web page on Data Protection: https://www.hud.ac.uk/informationgovernance/dataprotection/

  N.B. Any queries concerning the practical application of Data Protection should be directed to the University's Legal Secretary – Rebecca McCall. Email R.Mccall@hud.ac.uk.

- Confidential records
  Confidential/sensitive electronic records should be either password protected in shared areas or placed in K drives. They should not be kept on desktops or in 'My Documents'. Any confidential paper records should be kept in locked cabinets and access to keys restricted. Line Managers should manage records relating to their staff in this manner.

E. Destroying paper records

Amy-Jo Cameron-Williams
University Archivist and Records Manager

March 2018

- Shred financial/confidential paper documents/records
  Documents/records containing financial or personal data must be shredded, rather than recycled or binned.

Amy-Jo Cameron-Williams
University Archivist and Records Manager

March 2018