

Step 1: Planning

- Is this a small office move or a larger move involving several offices, a department or a whole building? If the latter, this will require a formal project
- Nominate appropriate person to oversee all information security/data protection issues during move
- Review processes to see if its possible to be less reliant on paper, USBs and hard drives in new office

Remember to:

- Report any Data Protection/Information Security Incidents to IGO
- Contact Estates & Facilities 0161 2752424 for any access issues e.g. locks
- Inform the post room of your new address

Documents that must be retained, not needed in new office:

- [Contact IGO to arrange transfer to Iron Mountain](#)

Step 2: Document Review

- Use [Records Retention Schedule](#)
- Are any of the documents historically significant? If yes, contact University Archivist (55306)
- Consider what will be needed going forwards

Items for Disposal:

- Paper documents past their retention should go into confidential waste bins, IGO can arrange additional collections with Restore Datashred
- Optical/mag media disposal – Restore Datashred
- Disposal of Hardware – use [ITS Disposal and Recycling Service](#)

Step 3: Moving

- Place files that are moving with you into labelled boxes and keep an inventory of boxes
- Access to highly restricted information should be restricted and accompanied when moved
- Only approved removal companies should be used
- Take hardware and backups with you – account for all devices
- Ensure information held on electronic devices is saved onto University storage
- Review [Safety Services guidance](#) regarding safe moving
- Check all office furniture for any documents left behind
- Check all vacated areas including basements and storage rooms

Office Moves - Data Protection Guidance

These guidance notes along with the flow chart are to assist with the safe and secure transfer of data during an office move. Personal data can easily be left behind or mislaid, causing harm and distress to the individuals affected, and possibly result in a fine for the University. The Information Commissioner's Office (ICO – UK data protection regulator) can and have given out fines to organisations for failing to protect personal data during office moves. There are examples of some of these fines at the end of the document.

To avoid such an incident occurring at the University, please consider the following points before co-ordinating an office move:

Planning

- Make a systematic and methodical plan for managing the transfer of information. Ensure all involved are familiar with the plan and briefed accordingly.
- Depending on the scale of the move, it may be necessary to treat it as a formal or informal project. The decant out of a whole building would require a formal project whereas the movement of one team to a different office would not.
- An appropriate person should be nominated to co-ordinate/oversee all information security/data protection issues regarding a move. This person can ensure that any necessary documents are completed and that processes are followed correctly. It may be necessary to delegate duties to designated supervisors and managers and all involved must take responsibility for the security of any personal data throughout the moving process.
- Where not moving an entire department, but perhaps supervising an individual leaving the University, and hence, their office, line managers should complete the [staff exit checklist](#) with the member of staff. This document also highlights the need to archive or securely dispose of personal data that staff used, stored, or had access to.

Document Review

- Use the opportunity to review the documents and records in use (in both electronic and hard copy). Review it against the [University's Records Retention Schedule](#) and HR Services' [Retention of Staff Records – Guidance for Managers](#) and securely dispose of data that is no longer needed. Review your processes and identify where you can be less reliant on paper going forwards.
- Start disposing of documents before the move – there is no point packing and un-packing documents which are no longer needed. University blue-bag paper recycling bins can be used provided that the papers do not contain Highly Restricted or Restricted information - examples of data in these classifications can be found [here](#). If unsure, err on the side of caution.
- If disposing of hard copy data which contains Highly Restricted or Restricted information, and a shredding machine is not available to use locally, or the volume is too great, then the University have a contract with Restore Datashred, who now handle all confidential data disposal. Further information on this can be found here: [Disposal of Confidential Material](#). Note that the consoles and white sacks must not be used to dispose of any disks, CD's or other media.
- Follow the guidance in the link above for information on disposal of these items. PC's, monitors, printers, etc., that are no longer required should be stored securely somewhere where they can be collected and disposed of in accordance with the [IT Recycle and Disposal](#)

Service. Before collection, ensure that any data stored on the device which might be needed in future has been transferred to University storage. IT Services can ensure that any confidential information is wiped and securely disposed of through the above service.

- Please ensure that any information stored on the hard drives of PCs and mobile devices or removable storage devices (including removable hard drives and USB storage) is backed up to University storage before moving, in case they are damaged or lost in transit.
- Review processes going forwards to determine whether USBs and hard drives are still required.
- If it is believed the information is historically significant and belongs in the University archive, then please contact James Peters (55306) for further advice and guidance.
- If there are documents that are not to be kept in office storage or able to be disposed of but **must be kept** elsewhere – the University has a contract with a company called Iron Mountain, a records storage company. They will transfer paper documents to be stored off-site. Retrieval of documents can be requested, but there is a fee for this.
- Enquiries regarding the use of Iron Mountain should be directed through the Information Governance Office (Tel: 0161 275 7789; e-mail information.governance@manchester.ac.uk) and more guidance can be found [here](#).
- Prepare an inventory of all the equipment in use. If the data is Highly Restricted, then the file, USB, laptop or other device must be encrypted. All devices should be accounted for. If it is not necessary to move them whilst containing data, securely delete the data before storing them securely for the office move. If they need to be transported containing data, be vigilant when doing so - double check everything on arrival that was packed away.

Moving

- Make sure all furniture is thoroughly checked and clear of documents – desk drawers, filing cabinets, etc. Documents must not be left behind. Furniture full of documents cannot be moved, so ensure they are emptied into suitable containers marked appropriately before removal and make a clear note where the documents are from (e.g. grey filing cabinet number 3, drawer 1) so they can be easily be replaced on arrival. Any lockable drawers should be secured and the keys clearly marked and stored securely. Keep an inventory of all items and boxes being moved with a list of what is in each box. It is also a good idea to have a copy of the inventory of what is inside the boxes within the box in case anything goes missing. Check that everything has been moved when you are in your new office.
- Thoroughly check all rooms that are being vacated – is there a basement, or storage area near the office that has previously been used to keep documents or is still in use? Again, do not leave data behind, ensure it is reviewed against the retention schedules and process accordingly.
- If the information is Highly Restricted (as defined by the [Information Classification SOP](#)) or otherwise sensitive, access to it should be restricted. It should be clearly labelled, stored securely and accompanied when moved.
- The person responsible for the safekeeping of records must make sure that retained records are transported and stored appropriately. Ensure that you have used an approved removal company, with whom we have a contract, do not use personal cars. If records will be lodged with another person, they must agree to accept responsibility and provide suitable safe storage facilities. This must be documented.
- On arrival at the new office, locate keys for locked drawers, desk and filing cabinets, etc.
- Ensure the necessary security is fitted to office doors. If this is not there, contact the Estates helpdesk (0161 275 2424) to arrange.
- Ensure all partners know the new location; ensure the post room have been informed of the new location.

- This Safety Services document can provide further guidance about safely moving equipment and materials: [Vacating or Occupying Premises](#).
- Any suspected data protection or information security related incidents that occur as a result of an office move should be reported to the Information Governance Office in the normal manner. Click here to go to the [Incident Reporting](#) page.

Examples of ICO Fines

In December 2019, the first official UK penalty under GDPR was issued to a pharmacy supplies delivery service. Doorstep Dispensaree were fined £275,000 for failing to secure several boxes of customer records containing details of the medical conditions they were receiving medication for. The boxes had been left in an outdoor area pending disposal but had been left when the business moved premises. They were discovered by a third-party, and although they were damaged, much of the personal data was compromised.

A monetary penalty notice of £185,000 was served on the Department of Justice Northern Ireland after a filing cabinet containing details of a terrorist incident was sold at auction – the Department were organising an office move, and all unwanted/unnecessary furniture was sold at auction. Unfortunately this particular cabinet had not been checked before leaving the office and contained information about incidents from the 1970's to 2005, injuries sustained by people as a result of terrorist activity, compensation given to families, address details, etc.

Kent Police were fined £100,000 by the ICO, after highly sensitive and confidential information, including copies of police interview tapes, were left in a basement at the former site of a police station and found by the purchaser of the building.