# Working From Home - Disposal of Confidential Documents

## Introduction

When working from home you should try to ensure that you work with electronic documents wherever possible. On the odd occasion where you have to deal with physical documents (print outs, forms etc) you will need to ensure that these are disposed of in the correct manner.

## What is confidential?

Any document which if made public before a certain period may breach **commercial confidentiality** e.g.

- Contracts;
- Tenders;
- Purchasing documents;
- Insurance documents;
- Unpublished accounting records; and
- Maintenance records.

Any record which may breach **intellectual property rights** e.g.

- Unpublished research material, manuscripts.

Any document which contains **personal/identifiable information about an individual** e.g.

- Job applications;
- Sick pay records;
- Medical records;
- Wages and salary records;
- Grant applications;
- Student records;
- Student or staff discipline records;
- Interview notes;
- Admissions records;
- Questionnaire or other data collected under an understanding of confidentiality;
- Correspondence or other documents that reveal the contact details or any financial details of a named living individual; and
- Correspondence or other documents which reveal personal details or pass comments on a named living individual.

## Handling and storing confidential records when working from home

The following should be considered when storing confidential documents at home:

- Store confidential documents in secure and, where possible, lockable location – e.g. a filing cabinet, desk drawer.

    - Cabinets should always be kept locked when not in use;

- Confidential documents should never be left in an open area such as on a desk or other work area.
    - The document should be returned to a secure location when not in use;

**Destruction of confidential documents when working from home**

When it comes to destroying confidential documents, the objective is to ensure that these documents can't be put back together. This will ensure that the information they contain can't be compromised in any way.

There are two factors that can prevent a document being reconstructed:

- The size of which the particles have been shredded to; and
- The total volume of individual documents being shredded at that time.

It is recommended that if you have documents that require confidential disposal you should collect all the documents in a secure location at home (a locked desk drawer or similar) and then bring these to Campus to place in the Confidential Waste console when you are next on site.

You should place all the documents in a sealed envelope clearly marked for 'Confidential Destruction' to ensure their safe transit to the console.

Please also consider how you transport the information e.g. paperwork should be locked in the boot of your car and taken straight home and locked up. There are many 'horror stories' of information being left in trains, buses, etc. so please keep paperwork, information and devices safe and secure no matter how you are travelling.

Sadly most home shredders are not of a high enough security standard to allow us to use them when working at home and it's very unlikely that you will be shredding a large number of documents.

If you do have to shred documents at home you will need to ensure that your shredder is a cross cut shredder capable of shredding to DIN level P-4: maximum cross cut particle surface area 160mm² with a maximum strip width of 6mm = 6x25mm. Please do not use "tape" style shredders which shred into long strips – these can be stuck back together by someone determined enough.

If you are unsure if your home shredder is of a high enough standard top comply with DIN level P-4 please retain your documents as recommended above or contact Governance Services for further assistance.

## Electronic files and your home device

If you are using your own equipment (laptops, phones, etc.) for work purposes please ensure that you do not download / process others' personal data (being processed on behalf of the University) onto that equipment. If you need to process personal data using your equipment log in using VPN or Virtual Desktop. If you do download personal data for which the University is the Data Controller then you must ensure that the equipment is securely and fully wiped/destroyed at the end of its life. See the 'Bring Your Own Device' Policy.

***Note***: Opening an attachment from Outlook when logged on using Office 365 (not through VPN/VD) is likely to store the document directly onto your device.

**See also:**

What is and what is not a confidential record
Destruction of Personal Data
Records disposal and use of consoles