

Policy on Removing Files for Remote Working

Department of Education

**Department of Further and Higher Education, Research,
Innovation and Science**

February 2021

VERSION CONTROL

Version Number	Date Modified	Change Made By	Description of Change
Version 1.0	September 2020	Geraldine Keane	Initial Draft
1.1	October 2020	Stephen McGrath	Additional info added
1.2	October 2020	Stephen McGrath	Amended to capture obs from various units
1.3	January 2021	Stephen McGrath	Amended to include DFHERIS

Table of Contents

1. Introduction.....4

2. Key Considerations5

3. Tracking Movement of Hard Copy Official Files.....5

4. Transporting Hard Copy Documents outside of Department Offices.....5

5. Handling/Accessing Documents at Remote Address ('home')6

6. Printing Files Remotely6

7. Disposing of documents6

8. Managing and Reporting Data Breaches6

9. Appendix 1.....7

10. Appendix 2.....8

1. Introduction

Due to Covid-19 more people are now working remotely. In accordance with GDPR, the Department's Data Controllers (PO's and equivalent) must continue to ensure that all personal data is handled in a safe and secure manner and it is the responsibility of all staff to protect personal and sensitive data in their possession. While the Department of Education and the Department of Further and Higher Education, Research, Innovation and Science (the Departments) encourage paperless working where possible, this is not always achievable.

Remote working poses additional risk and requires vigilance in protecting hard copy personal data. Personal data should only be removed from the office when essential to carry out required work. The same Data Protection principles we adhere to in the office apply at home or in remote working spaces.

Aspects of this policy may be adapted to accommodate officers who work in a dispersed environment (e.g. Inspectorate, NEPS) while maintaining the overall spirit and principle of the policy.

This policy will be kept under review and may be modified, updated or withdrawn by the Department's Management Board.

This policy should be read in conjunction with: [Data Protection Policy](#) and Information Security Policy and this [remote working guidance issued by the Office of the Data Protection Commissioner](#).

2. Key Considerations

There are a number of points to be considered regarding the removal of paper files from the office:

- i. Who has permission to take paperwork home
- ii. Whether records containing particularly sensitive information should ever be removed from the office
- iii. Whether only copies may be removed or whether originals can be removed – originals may be irreplaceable
- iv. Are full files required or will partial files suffice for the task at hand
- v. How the paperwork should be transported
- vi. Can the file be scanned to a secure electronic folder for electronic remote access
- vii. How the paper records should be treated in the remote working environment

3. Tracking Movement of Hard Copy Official Files

- i. In order to track the movement of Hard Copy Official files for remote working, each business unit within the Department must appoint a staff member as a Local Registrar. The Local Registrar will track the movement of files using the Register of Removal template below at Appendix 1.

In this context official files mean the full official record (e.g. a registered numbered file) of an issue or more significantly of an individual. Completion of the register is not required for ad hoc paperwork or other forms.

- ii. When each file is returned to the Department, staff must email the Registrar in charge of the Register with the file number and file name. The email must be copied to the Data Controller (PO's or equivalent).

4. Transporting Hard Copy Documents outside of Department Offices

- i. All staff transporting Department files/records must ensure they are moved to their new location in a secure manner, proportionate to the type of information contained. If using public transport, staff should be extra vigilant.
- ii. Files containing personal data must be transferred directly from the Department to the remote location. Files MUST NOT be left in unattended car boots, etc.
- iii. Similar precautions must be used for the return of files.

5. Handling/Accessing Documents at Remote Address ('home')

- i. Operating a clean desk policy is encouraged whether working in the office or remotely. This will develop awareness and practices to secure confidential and sensitive records while working from home. Make it a habit to file away all sensitive or confidential information when not in use.
- ii. When not being worked on, the paper files/records must be stored in a secure location within the home, proportionate to the information within the documents, accessible only to the authorised staff member. Take steps to ensure the security and confidentiality of these records, such as by keeping them out of sight and reach in a cabinet, drawer, or a locked room, taking care to ensure that they are not left somewhere where they could be misplaced, stolen or inappropriately accessed.

6. Printing Files Remotely

Printing work documents outside the office when working from home should be managed in accordance with this policy. Identical to the removal of hardcopies from the office, printing work documents can risk confidential information or personal data becoming inadvertently disclosed to parties who should not see it. In order to maintain the security of data, it is important that printing records remotely is avoided where possible and if unavoidable, is only done when essential to do so.

7. Disposing of documents

While there is access to shredders or confidential bins in our offices many employees will not have the same ability to deal with their documents in the same way in a remote working environment.

All staff should take particular care that any confidential information, or documents containing personal data, are disposed of correctly. If you do not have access to a shredder, please consider the necessity of printing. If printing is necessary then documents should be held securely until such time as they can be disposed of correctly, if necessary by returning them to the office and disposing of them in the shredders or confidential waste bins.

8. Managing and Reporting Data Breaches

Where documents are misplaced, stolen or otherwise fall outside the control of officials a data breach may have occurred. For further guidance and, where relevant, in order to report a data breach, please follow the link(s) below and fill out the relevant information

[Data Breach Policy](#)

[Data Breach Summary](#)

[Data Breach Risk Assessment Methodology](#)

[Data Breach Risk Assessment form](#)

9. Appendix 1

Delivery of Department's Critical Activities –
Register of Removal of Paper Files for Remote Working by Authorised Staff Members

Section / Area	
Data Controller	

[illegible]

Register to be maintained by Local Registrar

10. Appendix 2

Process steps for the removal of files for the purpose of remote working

- I. Staff member identifies essential files necessary for the completion of a task to be completed remotely.
- II. The person removing the files from the office completes the Register of Removal of Paper Files form (appendix 1).
- III. The Register of Removal of Paper Files form is shared with line manager and the manager can sign to authorise.
- IV. The Register of Removal of Paper Files form and the files will be shared with and examined by the nominated local registrar.
- V. If satisfied that the Register of Removal of Paper Files form details the files to be removed, the Registrar will approve the removal of files.
- VI. A copy of the Register of Removal of Paper Files will be held by both the Registrar and the colleague removing the files to track and manage the file(s).
- VII. Once the files are no longer required for the essential task, they will be returned to the office.
- VIII. On return, the Registrar will check the file's contents against the Register of Removal of Paper Files form to ensure that the return is complete.
- IX. If satisfied all files are returned, the Register of Removal of Paper Files form is signed by the staff member returning the files and acknowledged by the registrar.