

**Confirmation of Data Destruction**

The purpose of this document is to confirm the destruction of data processed as per the terms and conditions of the ISSDA Data Request Form for Research/Teaching Purposes and End User Licence. When ISSDA receives this signed ‘Confirmation of Data Destruction Form’ it confirms the end of the project. This form must be completed and returned to ISSDA no later than 7 days post project expiry date. Please return completed forms to issda@ucd.ie

|  |  |
| --- | --- |
| Lead Researcher first name \*  |  |
| Lead Researcher last name \*  |  |
| Research Organisation \* |  |
| Project Title \* |  |

\* Indicates required field

Guidelines for Data Destruction can be found in Appendix 1; all data must be destroyed once the purpose of the contract has been completed.

**A. Electronic Copies of Data and Derived Information**

This refers to electronic copies of data processed and/or stored on ALL devices (e.g., PDAs, desktops, laptops, hard drives, servers, etc.) throughout the entire duration of the project, including devices used by all team members with access to the data. All backups and snapshots must also be destroyed.

**B. Paper Records**

This refers to paper records on which data was provided to you by ISSDA or on which data was subsequently stored.

**C. Data in the Cloud**

If you have saved data in the cloud, data destruction options are completely dependent on your provider. Please follow your provider’s data destruction best practices. All backups and snapshots must also be destroyed.

**DECLARATION**

I declare that the information provided in this document is accurate, complete and correct. I declare that original media, copies and back-ups of the data, paper records, derived information and cloud records for this project have been destroyed and are non-recoverable as outlined in the Data Destruction Guidelines.

**1. To be completed by Research Organisation (**This may be signed by but is not limited to Head of School/College/Faculty/Department, Head/Dean of Research/Research Support)

**Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Role in Organisation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**2. To be completed by Lead Researcher**

**Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**3. To be completed by PI/Supervisor**

**Signed \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**PI/ Supervisor**

**Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Office Use Only**

**4. To be completed by ISSDA**

**Signed** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_\_\_\_\_\_\_**

**Administrator, Irish Social Science Data Archive**

**Date \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**APPENDIX 1: GUIDELINES FOR DATA DESTRUCTION**

The data and any copies (including data in the cloud/server folders, all backup and historical copies of the data) must be destroyed using a method of destruction that will render the data unreadable through the use of an appropriate mechanical, physical or electronic process and converted into such a form that cannot be reconstructed in whole or in part.

1. **Electronic Copies of the Data from ISSDA and Derived Information**

Electronic copies include all data obtained from ISSDA. This may include but is not limited to the following:

|  |  |
| --- | --- |
| * Derived data
 | * Analysis tables
 |
| * Working files
 | * Backup files
 |
| * Data on server (incl. cloud)
 | * Information generated by linking other information to the data
 |
| * Temporary files
 |  |

**Magnetic Media (e.g., Hard Drives, Magnetic Tape)**

Magnetic media are storage mediums on which digital or analog information is recorded as magnetic signals, such as computer hard drives, magnetic tapes, and floppy disks. For magnetic media and read-write media, either physical destruction or over-writing may be used.

*Over-writing* is a method used to clear data from magnetic media that utilizes a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located. To ensure that the original data is rendered irrecoverable, the areas of the disk holding the data must be over-written, several times, with random data. The number of overwrites required depends on a number of factors, including the drive type and file system format, but typically, in order to defeat all but the most sophisticated of forensic recoveries, three passes is usually sufficient. Secure erasure programmes such as [Erasure](https://eraser.heidi.ie/) can be used to overwrite files.

*Physical destruction* is the preferred sanitization method because this ensures that data can never be recovered. Mechanical shredding and incineration are such measures used for disposition of sensitive data.

*Please note* that "regular" deletion of files is not adequate (including the "Empty Trash" feature) - the data still exists on the disk; it is merely the index pointers to the data which are removed in such an operation.

1. **Paper Records**

Paper records should be destroyed in a manner that leaves no possibility for reconstruction of information. The appropriate method for destroying paper records is cross-cut shredding.