NISRA - RSU
NORTHERN IRELAND STATISTICS & RESEARCH AGENCY
RESEARCH SUPPORT UNIT

Research Support Unit

RSU070 – RSU Policies

Background

Once a project has been approved the following policies must be read and the RSU Project Agreement document signed before any data extracts will be created for researcher use:

- Research Support Unit Security Policy
- Research Support Unit Disclosure Control Policy
- Research Support Unit Licence Agreement
- Census Confidentiality Undertaking

NISRA - RSU
NORTHERN IRELAND STATISTICS & RESEARCH AGENCY
RESEARCH SUPPORT UNIT

RSU Security Policy

Background

Researchers are able to obtain access to de-identified data in a safe manner via access to a secure environment within NISRA. The secure environment, which is governed by protocols and procedures to ensure data confidentiality, is managed by the NISRA Research Support Unit (RSU).

1. Due to the highly sensitive nature of the data, it is extremely important that strict security guidelines are in place and adhered to at all times, ensuring that the data is held and processed within all legislative boundaries. This is summarised in two overriding security principles under which the NISRA RSU operates. These are:
   (i) no physical or electronic media with individual level identifiable data will leave the secure environment of the Research Support Unit within NISRA headquarters without the prior approval of the Registrar General; and
   (ii) all data processed within the secure environment will be managed and handled according to the relevant regulatory and statutory principles and will be processed for statistical and research purposes only.

2. The remainder of this document details the RSU security guidelines under the following sections:
   - Access to the Data;
   - Location of Access;
   - Access Prerequisites and Methods;
   - Outputs; and
   - Post-project Procedure.

Access to the Data

3. On the approval of a research project application, the RSU team will extract the specified data as detailed in the project application and produce a bespoke dataset. Access to this dataset will be restricted to:
   - Researchers listed in the Application Form that have completed an RSU Project Agreement form;
   - Additional researchers added via a Project Modification;
   - Research Support personnel; and
   - NISRA data management staff.

4. In the event of a change in research personnel or the requirement of additional data outside the scope of the original application, an amendment should be made to the Application Form as appropriate and resubmitted for approval to the appropriate approvals group. The Research Support Officer will help ensure that this process is carried out with minimal delay to research progress.

Location of Access

5. All data access must be carried out in the RSU secure environment within NISRA headquarters.

6. Access to the secure environment is strictly by appointment only and all visitors must report to reception on entry. Appointments are subject to availability and should be made to RSU staff with at least one days notice given. Data access is usually available between 8.30am and 4.30pm Monday

to Friday. However, this cannot be guaranteed and is dependent on the availability of supervisory staff.

7. Due to current COVID-19 regulations, access to the NISRA secure environment is restricted. Researchers must not arrive at Colby House without the prior authorisation of RSU. Researchers should submit an RSU Secure Environment Booking Form to RSU by the Wednesday of the current week for bookings the following week. Booking slots will be allocated fairly amongst researchers and will follow social distancing guidelines. All researchers attending Colby House are expected to adhere to all on site protocols. A continued opening of the secure environment will be dependent on the availability of staff and future potential lockdowns therefore it is possible that sessions could be cancelled at short notice.

8. Access to the secure environment is via a security pass which is restricted to RSU authorised personnel only.

Access Prerequisites and Methods

Documentation

9. Prior to accessing the data, all researchers (and their Head of Proposed Study) must sign the RSU Project Agreement to confirm that they have read and understood all necessary documentation to comply with statutory and regulatory rules relating to data protection and privacy. This documentation includes:
   - RSU Security Policy;
   - RSU Disclosure Control policy;
   - RSU Licence Agreement;
   - NILS Publication Policy (for NILS projects only); and
   - Census Confidentiality Undertaking

   Researchers will not be given access to the secure environment or research data before a signed copy of the RSU Project Agreement is received by the RSU team.

IT

10. Access to data will be made via a terminal on the Research Network in the secure environment.

11. Researchers will be given a user name and temporary password by the system administrator. This password must be changed at first login. Where a researcher is working on more than one project, a separate login will be issued for each project. Passwords should not be divulged to other researchers (even those working on the same project) under any circumstances.

12. On accessing the network, users will have access to a shared folder which will contain their project specific data. All research work must be stored in this folder, as any work stored on the terminal hard drive will be lost during routine data formatting processes.

13. Should a researcher wish to have files transferred to their project folder, these should be sent via email to NISRA RSU. For security reasons, files cannot be transferred directly onto the Research Network from portable data storage devices such as USB drives, CDs, etc.

14. All data reading and extraction facilities (USB ports, CD/DVD Writers, Card Readers, wireless connections etc.) have been disabled on the research terminals and no attempt should be made to reactivate them.

15. Use of personal electronic devices within the secure environment is strictly prohibited. This includes, but is not limited to, laptops, mobile phones, all music devices and digital photographic equipment.

16. By default, permitted access onto the network for research is restricted to between 8.30am and 4.30pm Monday to Friday. In some circumstances, on request, other times may be facilitated subject to the availability of suitable supervisory staff. An audit of all logon attempts (success and failure) are recorded and routinely checked for unauthorised access.

17. Request for access to the internet (on a separate PC not connected to the RSU network) will be considered on a case by case basis. Any internet access will be restricted and supervised to ensure no breach of the security and disclosure policies.

Other

18. Whilst at a research terminal, all researchers must not copy information electronically in any format or media or remove manually copied paper information. All written notes should be made within the coloured file pads supplied by RSU and are not to be removed from the secure environment. Written notes can be retrieved for use on each visit.

19. All researchers must be supervised at all times by RSU staff. On some occasions a researcher may be asked to leave the secure environment if suitable supervisory cover is unavailable. RSU staff will endeavour to avoid such circumstances.

Outputs

20. Under no circumstances will individual level information leave the secure environment. All data to be released from the secure environment must comply with the RSU Disclosure Control Policy and the RSU Licence Agreement.

21. Researchers requesting the release of data must complete a copy of the Intermediate Outputs Clearance Request Form stored within their Project Folder or available on the NILS-RSU website.

22. The requested data will then be checked by a Research Support Officer to ensure compliance with the RSU Disclosure Control Policy. The cleared outputs will then be securely forwarded to the researcher.

23. Further steps to ensure no unauthorised access of an output during the transfer of data to researchers may be considered in the future. These may include:
    - Data being transferred via email to a researcher may be encrypted using 256 bit AES encryption software, for example using WinZip (version 9 or greater). In such cases, a password will be required to extract the files;
    - In certain circumstances, the Head of Demographic Statistics will consider requests for data to be transferred via writable media (CD, DVD, etc.). If approved, the data will be encrypted using the method outlined above and will be sent via special delivery. The cost of this will be covered by the researcher.

Post-project Procedure

24. Following the completion of a project, all data and analyses contained within the corresponding project folder will be archived and securely stored by the Dial team.

25. Logon identities and scripts for researchers relating to the project will be cleared and all access will cease.

26. Further requests for information from the folder or for further access for analysis relating to the project will only be allowed in line with the NILS Archiving Policy.

NISRA - RSU
NORTHERN IRELAND STATISTICS & RESEARCH AGENCY
RESEARCH SUPPORT UNIT

RSU Disclosure Control Policy

NILS and ADRC data is managed by the Northern Ireland Statistics and Research Agency (NISRA) and access to the data is restricted to within the secure environment in NISRA headquarters. Any person using NILS or ADRC data, either in the capacity as a Research Support Officer or researcher, must comply with all confidentiality requirements detailed in the RSU Licence Agreement and the RSU Security Policy.

In addition to the confidentiality protocols, certain disclosure control measures will be applied by RSU personnel to all output information released. This is to ensure that no individual can be identified within the data. If data are to be released in tabular form, then the Research Support Officer must ensure that any information that could potentially identify an individual is aggregated, suppressed or removed as appropriate. The disclosure control protocol includes:

- When releasing tabular data, research support personnel must ensure that cell counts are 10 or greater. If associated data allows the cell to be split then the Research Support Officer must aggregate the data to the highest level consistent with the need to explain the results.
- Sample uniques or individual cases are never allowed.
- For NILS projects, no data on birth dates of NILS members may be released, with the exception of year of birth. Any analyses which require month of birth or full date of birth will be conducted by NILS-Core staff.
- For NILS projects, no data on date of death of NILS members may be released, with the exception of month and year of death. Any analyses which require day of death will be conducted by NILS-Core staff.
- Exposure times may be included in aggregated datasets provided there is more than one event in each cell.

The following types of data are not routinely released but will be considered by NILS support personnel on a case-by-case basis. (Note the turn-around time for these types of data may take slightly longer than would generally be the case.)

- Reporting residual values
- Scatter diagrams - particular care should be exercised with extreme values.

Further restrictions will also be placed on the release of any variable considered to be sensitive. These include variables relating to small numbers of people in Northern Ireland (i.e. local-area geographic identifiers, detailed ethnicity, rare causes of death etc.). Other variables, such as religion, may also be treated as sensitive, depending on the context of the research. It should be noted that selection criteria used in extracting data such as sex and age may be disclosive when used in conjunction with other variables.

**Researchers should note that further restrictions relating to the release of outputs may be put in place by Data Controllers. These are entirely at the discretion of the Data Controller, and refusal to accept any additional conditions may result in access being withdrawn.*

Researchers are not permitted to difference tables which may lead to the production of disclosive cell counts. It is the researcher's responsibility to:

- consider whether outputs are required outside the RSU secure environment; and
- remove any potentially disclosive information prior to submitting outputs for disclosure checks and transfer.

If a Research Support Officer believes that data may be disclosive they will either remove the table or advise the researcher to aggregate the data further.

NISRA - RSU
NORTHERN IRELAND STATISTICS & RESEARCH AGENCY
RESEARCH SUPPORT UNIT

RSU Licence Agreement

1. Where on-site access to data at the Northern Ireland Statistics and Research Agency (NISRA) is required for this project I agree to comply with any conditions for data access required by the NILS Research Approvals Group (RAG)/Administrative Data Research Centre for Northern Ireland (ADRC-NI).

For those receiving intermediate outputs:

2. The intermediate outputs supplied to me will be used only for the approved research project identified in the associated Application Form.

3. The intermediate outputs will not be released to any other individual(s) or organisation(s) not named on the approved Application Form. Everyone mentioned on the Application Form has signed an RSU Licence Agreement.

4. Additional project contributors or named associates will only be allowed access to the intermediate outputs or any information derived from the intermediate outputs after a Project Modification has been approved, and the additional researcher has signed a separate Licence Agreement.

For all outputs:

5. I will submit outputs to NISRA Research Support Unit (RSU) for clearance before releasing them for publication or to anyone who has not signed a Licence Agreement for the project. All final outputs will acknowledge support of the RSU and include a conventional disclaimer.

6. I will not use outputs supplied to me to attempt to obtain or derive information relating specifically to an individual or household, nor claim to have obtained or derived such information. Where there is doubt about the implications of a particular situation, the advice of NISRA will be sought. If, subsequent to release, it appears possible that there is a risk of disclosure, NISRA will be informed immediately.

7. In the case of NILS Distinct Linkage Projects using anonymised/pseudo-anonymised service provider data in the secure environment any research output that directly brings focus on an individual GP practice will not be allowed. The RSU Disclosure Control Policy will apply but in addition all outputs will be scrutinised by senior members of staff.

8. Outputs or files derived from them may only be used for the approved project. Any request for an extension to the approved project must be submitted to the RSU on a Project Modification Form.

9. The focus of the project is statistical research/analysis and the data will not be used for any other purpose, including personal or commercial gain.

10. There will be no matching or linking of the intermediate outputs to other data sources beyond those described in the approved Application Form.

11. The Licence Holder agrees to comply with any additional conditions that the Approvals Panel or Data Controllers may consider necessary. Such conditions will be sent to the Licence Holder when the application is approved. Accessing of the data by the Licence Holder will signify acceptance of such additional conditions.

12. All members of the research team involved in this project understand that the breach of any of the provisions of the Licence Agreement may result in sanction being sought against those named on the Application. These may include legal proceedings taken by NISRA for breach of obligations under statute or common law. Details of the penalties that may be applied can be found in the General notes section below.

13. The Licence Holder is required to report promptly a breach of any of the terms of the Licence Agreement. Failure to disclose details is a fundamental breach of this Licence.

14. Any disputes arising from the use of the data and/or the terms of the Licence Agreement will be resolved initially between NISRA and the Licence Holder (or the organisation with ultimate responsibility for the Licence Holder). Otherwise, outstanding issues will be referred to the Registrar General.

General notes:

Definitions:
Intermediate outputs – are outputs that are released to researchers following disclosure checks for the purposes of writing up results, or discussions with other project team members. Intermediate outputs include all files released from the secure environment, including aggregated datasets, frequency listings and cross-tabulations, summary statistics, regression coefficients, log files and graphical outputs. Intermediate outputs are not cleared for publication.

Final outputs – are the drafts (early & final) of papers, presentations, tables for publication etc.

Licence Agreement

1. The Licence is required for access to data in the NISRA secure environment and the release of intermediate outputs from the NISRA secure environment.

2. Approval to access the data is conditional upon the Licence Holder and Head of the Proposed Study agreeing to the terms and conditions detailed in the NILS Licence Agreement.

3. NISRA retains the right of veto and may refuse access to the data requested by the Licence Holder. Any such decision will be communicated to the Licence Holder, together with the reason for the decision.

4. A Licence Agreement is to be signed by all researchers named on the Application Form (or any subsequent Project Modification Form), along with their Head of Proposed Study/Lead Researcher. Where the researcher is a student their supervisor must be included in the research team.

5. Parties to this Licence, who will be bound by the terms of the Licence, include the:
   (i) Researchers named on the Application Form (or any subsequent Project Modification Form); and
   (ii) Northern Ireland Statistics and Research Agency (NISRA).

6. The terms and conditions set out in the Licence Agreement may be subject to change. In the event of any such change, the Licence Holder will be required to sign a new version of the Licence Agreement. It is not anticipated that any such changes will result in a delay to the access process.

7. The principles of the Freedom of Information Act apply to this Licence Agreement and nothing provided in this Licence is confidential to the Licence Holder or to NISRA. To disclose the details of the Licence Agreement would not be a breach of any duty of confidence and therefore the details

would be made available to the public on request and may be included as part of the metadata attached to any of the outputs arising from the access.

8. The Licence Holder guarantees to preserve the confidentiality requirements of the intermediate outputs at all times. The Licence Holder will ensure that:
   (i) Data may only be accessed according to the security conditions detailed in the RSU Security Policy; and
   (ii) Data requested under this Licence Agreement will only be accessed within the NISRA secure environment.

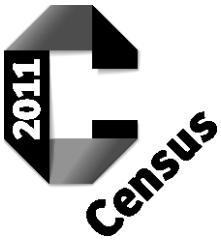
9. The Licence Holder is reminded that a breach of any of the terms of the RSU Policies (RSU070) must be reported promptly to NISRA. Failure to do so is a fundamental breach of the Licence.

10. A breach can be a breach of procedure or a breach of data.

    In the event of a breach of procedure, the NISRA sanctions that may be applied are:
    (i) An individual's breach would, as a minimum, result in the requirement that the individual repeats Safe Researcher Training. In addition the individual may be required to repeat and pass the online Safe Researcher Training assessment.

    In the event of a data breach or a repeated breach of procedure, the NISRA sanctions that may be applied are:
    (i) For a first offence, depending on circumstances, the penalty should be a maximum 12 month non-discretionary suspension from access to any NISRA micro-data, applicable to the individual in question. Other research data centres will be notified as appropriate (i.e. ADRC-England, ADRC-Scotland, ADRC-Wales, ONS LS, SLS). Depending on the seriousness of the breach, the termination of access may be permanent.
    (ii) An individual's second breach would, as a minimum, result in a suspension of access of more than 12 months, or permanently, on the individual, and would generate a written warning from the Registrar General.
    (iii) The Registrar General may decide any discretionary penalty, including permanent suspension for the individual and/or pursuing in the Courts an action for breach of contract.
    (iv) A breach under the Digital Economy Act may result in a penalty of up to two years, imprisonment, a fine, or both.

    The consequences of any suspension of access (such as consequent inability to honour research contracts) will not be taken into consideration when applying minimum penalties or any of the Registrar General's discretionary penalties.
    Any appeal will be to the Registrar General only.



CENSUS CONFIDENTIALITY UNDERTAKING
(Northern Ireland)

All persons accessing census-level micro data within the NISRA secure environment are subject to the confidentiality requirements for personal Census information in accordance with the Census Act (Northern Ireland) 1969, as amended by the Census (Confidentiality) (Northern Ireland) Order 1991. Breaching these requirements could result in a criminal record and a fine and/or up to two years imprisonment.

Background

Improper handling of personal Census information could breach the privacy of an individual and damage public trust in the Census. Everyone working on the Census is therefore required to make a **Confidentiality Undertaking** that they fully understand their legal obligations and are aware of the penalties for unlawfully disclosing confidential Census information.

The relevant parts of the Census Act (Northern Ireland) 1969, as amended by the Census (Confidentiality) (Northern Ireland) Order 1991 are listed below and can be read in full at:

http://www.opsi.gov.uk/RevisedStatutes/Acts/apni/1969/capni_19690008_en_1
http://www.opsi.gov.uk/si/si1991/Uksi_19910760_en_1.htm

Extracts from Sections 6 and 7 of the Census Act (Northern Ireland) 1969, as amended by the Census (Confidentiality) (Northern Ireland) Order 1991 are listed below.

Section 6 states:

6 (1) Information obtained for the purposes of a census under this Act shall not be used otherwise than in accordance with this Act.

6 (3) Any person having the custody, whether by himself or on behalf of any other person, of any forms of return, enumeration books or other confidential documents relating to a census taken under this Act or any Act passed before the passing of this Act shall not permit any other person without lawful authority to have access thereto.

Section 7 states:

7 (1) If any superintendent, enumerator, or other person employed under this Act makes wilful default in the performance of his duties under this Act or any order or regulations made or instructions, there under, he shall be guilty of an offence and for each such offence be liable on summary conviction to a fine not exceeding level 3 of the standard scale.

(4) If a) the Registrar General or any person who is under his control, or a supplier of services to him; or b) any officer of the Department of Health and Social Services or any person acting on behalf of that Department; uses, without lawful authority, any personal census information or discloses, without such authority, such information to another person, he shall be guilty of an offence.

(5) If any person uses any personal census information which he knows has been disclosed in contravention of this Act or discloses such information to another person, he shall be guilty of an offence.

(7) A person guilty of an offence under subsection (4) or (5) shall be liable

a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both;

b) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

(8) For the purpose of this section

a) a person is to be treated as under the control of the Registrar General if he is, or has been (i) employed by the Registrar General (whether or not on a full-time basis); or (ii) otherwise employed, or acting, (whether or not on a full-time basis) on behalf of, or as part of the staff of, the Registrar General for the purposes of this Act;

b) a person is to be treated as a supplier of services to the Registrar General if (i) he supplies, or has supplied, any services to the Registrar General in connection with the discharge by the Registrar General of any of his functions; or (ii) he is, or has been, employed by such a supplier.

Document Management

Access Limitations:	None
Maintainer:	RSU
Document Identifier:	RSU070
Replaces:	NISRARSU042
Review period (months):	24 Months
Is related to:	RSU071

Version History

Version	Notes	Last Amended
1.2	Update to booking requests to secure environment via booking form prior to visit 7.	17/08/2021
1.1	Minor updates to RSU versions in text HB	14/05/2021
1.0	Document Re-Numbered	22.12.20
0.2	Licence Agreement sanctions updated (CMcL)	12.11.2018
0.1	Created by RSU (CMcL)	May 2017