SECURE LAB BREACHES PENALTIES POLICY

PUBLIC VERSION

2 JANUARY 2014

T +44 (0)1206 872251
E rwelpton@essex.ac.uk
ukdataservice.ac.uk

UK DATA ARCHIVE
UNIVERSITY OF ESSEX
WIVENHOE PARK
COLCHESTER
ESSEX, CO4 3SQ

WE ARE SUPPORTED BY THE **UNIVERSITY OF ESSEX**, THE **ECONOMIC AND SOCIAL RESEARCH COUNCIL**, AND THE **JOINT INFORMATION SYSTEMS COMMITTEE**

Contents

List of Tables

Scope

This document outlines the penalties for breaches of the terms and conditions of use of the UK Data Service Secure Lab. Background information is provided concerning the agreements that users of the service enter into and the legal framework that underpins those agreements. The policies stated herein apply to users of the UK Data Service Secure Lab, and to UK Data Service staff.

Definition of Terms

"ONS Approved Researcher"

> a researcher to whom the UK Statistics Authority, under the Statistics and Registration Services Act (SRSA) 2007, has granted access to Personal Information held by it for the purposes of statistical research

"ESRC Accredited Researcher"

> a researcher to whom the UK Data Service and the data owner(s) have granted access for the purposes of statistical research to Personal Information not held by the UK Statistics Authority and which have been licensed to the UK Data Archive/University of Essex for dissemination

"Personal Information"

> information that relates to and identifies an individual (including a body corporate) taking into account other information derived from published sources

"End User Licence" (EUL)

> the agreement entered into by a researcher when registering to access data from the UK Data Service (see *End User Licence)*. Researchers who access data via the Secure Lab necessarily agree to the EUL as they must register with the UK Data Service during the process of applying for access.

"Declaration" of the ONS Approved Researcher or ESRC Accredited Researcher application

> this declaration is signed by a researcher when completing either the ONS Approved Researcher or ESRC Accredited Researcher application. Briefly, the researcher declares that they understand the terms and conditions of the licence under which they apply for access.

"Secure Access User Agreement"

is signed by the researcher (and by a representative of their institution). By signing this agreement, the researcher agrees to extra terms and conditions of use associated with the Secure Lab, additional to the EUL and the Declaration.

Higher Education (HE) researchers

researchers who are employed or study at a UK Higher Education Institution (for example, a University). The researcher access the Secure Lab (remotely) from this institution.

Non-Higher Education (non-HE) researchers

researchers who are granted access to data via the Secure Lab but whom are not employed (or study) at a University. Instead, they are employed at an ESRC-funded Research Institute (for example, the Institute for Fiscal Studies.

Commercial Research

research is defined as commercial "where a direct objective is to generate revenue and/or where data are requested for sale, resale, loan, transfer, or hire", see http://ukdataservice.ac.uk/get-data/how-to-access/registration.aspx/tab-commercial-users, 2nd January 2014.

Data Owner

an organisation that collects data and passes the data to the UK Data Archive for dissemination.

1. Introduction

A user of the UK Data Service Secure Lab (hereafter 'Secure Lab') is required to register with the UK Data Service, thereby agreeing to an EUL and to be either an "ONS Approved Researcher" or an "ESRC Accredited Researcher". The term AR, used elsewhere in this document refers to both of these types of user.

We believe that if there is user understanding of the nature of, and reason for, penalties for breaches (which either constitute non-compliance with their Secure Access User Agreement and other UK Data Service standards as explained at their training, or more serious incidents which could lead to the disclosure of personal information), we will avoid the inadvertent malpractice that social science researchers are most likely to be prone to. Therefore, ARs are additionally only able to use the Secure Lab if they have signed a Secure Access User Agreement and successfully completed mandatory face-to-face training (see *Authorisation Process*).

The Secure Access User Agreement outlines the terms and conditions of use of the Secure Lab and is signed by the AR and a senior member of their institution. The agreement includes a) liability for the user to complete the Secure Lab training; b) information security responsibilities; c) penalties and breaches; d) output release policy; e) acknowledgements and copyright requirements. The agreement demonstrates that the prospective user understands the seriousness of the undertaking and that they and their institution understand the penalties that may be imposed for breaches of security or confidentiality.

Mandatory training allows the UK Data Service to ensure that ARs are fully aware of any penalties which they might incur if they cause a breach.

All UK Data Archive staff are required to agree to the EUL and to sign a non-disclosure agreement that would be applied in case of a staff breach. Staff are made aware of the contractual penalties which might arise from a breach of a data deposit licence and of the criminal penalties which might arise from a breach of the Statistics and Registration Services Act.

The UK Data Service reserves the right to temporarily or permanently withdraw access to the service if it believes that any user is perpetrating or attempting to perpetrate any of the breaches listed in the Table in Appendix A.

The UK Data Service has discretionary powers over the application of penalties for self-reported breaches.

- Application of the penalties for intentional breaches discovered by the UK Data Service is non-discretionary. The penalties for such breaches (shown in the table of offences and penalties below) are a fixed tariff.

- Self-reported unintentional breaches will be penalised with discretion; if a penalty is to be applied the relevant tariff (shown in the table below) will be considered a maximum only. Researchers who take full and prompt action to correct a self-reported and unintentional breach will not normally be penalised but may be asked to repeat training/induction. Penalties for repeated self-reported but unintentional breaches will increase with each breach committed.

2. Penalties under the Act

The SRSA 2007 Act states that a person who discloses Personal Information "is guilty of an offence and liable — (a) on conviction on indictment, to imprisonment for a term not exceeding two years, or to a fine, or both; (b) on summary conviction, to imprisonment for a term not exceeding twelve months, or to a fine not exceeding the statutory maximum, or both." [1]

However, this subsection of the Act does not apply when the person making the disclosure "reasonably believes" that either Personal Information is not specified in the information which is disclosed, or that a person's identity cannot be deduced from the information, or that a person's identity can not be deduced from the information taken together with any other published information.

Nevertheless, the removal of Personal Information from the secure confines of the Secure Lab remains a breach of the Secure Access User Agreement (section 19), regardless of whether a user had 'reasonable belief'. Users are advised in the training course that they should only regard the statistical outputs (publications, presentations etc) which they have received from a UK Data Service member of staff, to be non-disclosive, and that receiving such an output from a UK Data Service member of staff is their 'reasonable belief'.

Secure Lab users of ONS Personal Information are made aware through training and service documentation that ONS has stated that it will always seek prosecution for any breach of the SRSA 2007. The only exceptions are where the disclosure was unintentional and self-reported, or the 'reasonable belief' defence is unambiguously relevant. However, the reasonable belief defence is effectively removed by Secure Lab training (see *Secure Access Training Modules*)).

3. Non-compliance for Secure Lab Users

The following agreements apply to Secure Lab users:

- End User Licence;

- Approved/Accredited Researcher declaration;

- Secure Access User Agreement, which requires an institutional signature, in order to ensure the institution is aware of the penalties to which it may be subject in the event of a breach.

The above agreements can be characterised as an order of incremental gravity. By signing the Secure Access User Agreement, the researcher is agreeing to terms and conditions specific to the Secure Lab that are in addition to the terms and conditions of the EUL. Owing to the confidential nature of the data accessed via the Secure Lab, breaching the terms and conditions of the User Agreement could have serious consequences for the researcher, including legal ramifications.

A series of additional penalties for breaches will come into force when the AR declaration and the Secure Access User Agreement are signed. The majority of these breaches are procedural and can be dealt with by the UK Data Service with no additional input from the data owner (although data owners will be notified that a

[1] Statistics and Registration Services Act 2007 § 39 (9).

breach has occurred see *Secure Access Information Security Event Response Procedures).* However, the severest offences will be dealt with more rigorously..

3.1. Commercial use of data

For the purposes of the initial service, researchers will not be allowed to use any data or data outputs, regardless of their origin for *any* commercial exploitation, as the licence held by the UK Data Archive with software suppliers will be broken. This issue may need to be addressed further in the future.

Defining 'commercial' purposes can be problematic. ONS allows statistical research that generates commercially viable statistical products. Unlike research for publication or for use in the formulation and development of public policy, Crown Copyright requires that the appropriate 'click-use' licence is obtained by the research organisation that seeks to commercially exploit a statistical product derived wholly or in part from government data. Under the terms of a click-use licence a royalty on the commercial value of the statistical product may be payable to the Office of Public Sector Information. However, the selling on of data or outputs for personal financial gain and the use of the Secure Lab by researchers acting as paid 'agents' of businesses for whom the Secure Lab was not designed nor funded is not permitted.

Examples of commercial use of data (and therefore not permitted) include:

- Using the data for commercial research
- Selling data or outputs for personal financial gain
- Acting as paid 'agents' of businesses for whom the Secure Lab was not designed nor funded

4. Right of appeal

The right to an internal appeal is allowed. Thus all appeals should be to the stakeholder with the highest level of involvement with the offence.

If a researcher considers a penalty following a self-reported unintentional disclosure is unfair, the right of appeal is to the organisation(s) with the primary responsibility for enforcement (as detailed in the table of offences and penalties below).

A. Appendix: Offences and Penalties

The purpose of this list of penalties is to have a deterrent effect, and act as a reference for users, who should be aware of the consequences of breaching their User Agreement or any procedure prescribed by the UK Data Service. Punishment is not the primary objective.

In this table AR is used to denote both (ONS) Approved Researchers and (ESRC) Accredited Researchers.

The penalties listed below, *for intentional discovered breaches,* are non-discretionary. The penalties for such breaches are a fixed tariff.

For *self-reported unintentional breaches* the penalties listed below will be considered to be a maximum, and will be applied with discretion. Researchers who take full and prompt action to correct an unintentional breach and who report the breach and their actions will not normally be penalised but may be asked to repeat training/induction.

This table provides a list of the main offences and penalties. Penalties may be imposed at the discretion of the UK Data Service for other offences not listed here that are considered to breach the terms and conditions of the use of the service.

Under the agreements that apply to Secure Lab access, researchers agree to inform the UK Data Service of any publications (external conferences, journal articles, reports) using outputs from the Secure Lab and also of any errors found in the data or enhancements made to the data. Whilst there is no formal penalty for not informing the Archive, as part of the Secure Lab community researchers are expected to share this information – researchers are regularly followed up and contacted by the UK Data Service to provide such information. If researchers do not provide such information, the UK Data Service reserves the right to take appropriate action.

It should be noted that whilst survey respondents are not the owners of the data for the purposes of this document, they have the right to take independent civil action against any offender who damages them by release of their Personal Information.

A breach of procedures (i.e. a violation of the licence), will be dealt with by UK Data Service. Where relevant data legislation has been abused (a violation of statutory law), the UK Data Service will assist the relevant data owner, should the said organisation wish to make a prosecution. A procedural breach could occur that may or may not result in a criminal offence being committed, depending upon whether personal or confidential data is mishandled. For example, removing statistical outputs without the permission of the UK Data Service is a breach of procedures: where this action results in confidential data removed from the Secure Lab, then a criminal offence may have been committed.

Table 1: Table of Offences and Penalties

Offence	Expected Penalty	Notes/example	Primary responsibility for enforcement	Type
Applying for AR status without intent to use data	First offence 12 month ban on application Second offence 2 year ban on application Third offence permanent suspension	This does not apply to researchers who apply to use the data for a valid project that is then, for example, cancelled.	UK Data Service	UK Data Service Rules
Using the service and/or data for commercial purposes	First offence 12 months access suspension Second offence 2 years access suspension Third offence permanent suspension Depositor may impose additional penalties.	See section 4.1 of this document.	UK Data Service/Depositor	UK Data Service Rules Licence violation (Civil Offence)

Incorrectly attributing copyright or other rights to oneself	First offence 12 months access suspension Second offence 2 years access suspension Third offence permanent suspension Depositor may impose additional penalties.	Refer to acknowledgement and copyright section of the SDS User Agreement.	UK Data Service/Depositor	UK Data Service Rules Licence violation (Civil Offence)
Infringing safe environment rules	First offence 2 years access suspension Second offence permanent suspension	Including the copying of statistical results from the screen without submitting to the UK Data Service for statistical disclosure control	UK Data Service	UK Data Service Rules
Attempting to infringe security requirements	First offence 2 years access suspension Second offence permanent suspension	See ‘infringing security requirements’ below..	UK Data Service	UK Data ServiceRules
Transferring log in details to any other user	First offence 2 years access suspension Second offence permanent suspension	This includes sharing login details (whether username, password or both) with someone else, even someone working on the same project or a supervisor.	UK Data Service/Depositor (if ONS)	Licence violation (Civil Offence)
Providing disclosive code used to others without authorisation	First offence 2 years access suspension Second offence permanent suspension	This includes syntax files that might include identifiers, such as IDBR reference number or summary statistics.	UK Data Service/Depositor (if ONS)	Licence violation (Civil Offence)
Providing false information on the AR Form or Declaration	Permanent suspension		UK Data Service	Licence violation (Civil Offence)
Altering the AR Declaration	Permanent suspension		UK Data Service	Licence violation (Civil Offence)
Attempt to access datasets to which not authorised	Permanent suspension		UK Data Service	Licence violation (Civil Offence)
Attempt to use data for purpose not specified in the application	Permanent suspension	An example includes using data obtained under an approved project for a new research project that has not been approved.	UK Data Service/Depositor if ONS	Licence violation (Civil Offence) / Violation of Statutory Law (Criminal Offence) for ONS data

Attempt to use data for other than statistical research	Permanent suspension		UK Data Service/Depositor if ONS	Licence violation (Civil Offence) / Violation of Statutory Law (Criminal Offence) for ONS data
Sharing any data outputs which have not been approved	Permanent suspension. NB sharing data outputs which prove to be disclosive will be subject to more severe penalties.		UK Data Service/Depositor if ONS	Licence violation (Civil Offence) / Violation of Statutory Law (Criminal Offence) for ONS data
Infringing security requirements	*Expected Penalty for HE researchers* a) Permanent suspension (individual); AND b) 1 year suspension (institution) AND c) 2 year sanction from ESRC funding (individual) AND d) 1 year sanction from ESRC funding (institution) *Penalty for HE researchers* a) Permanent suspension (individual); AND b) 5 year sanction from ESRC funding (individual)	This includes, for example, not keeping login secure, not keeping anti-virus software uptodate, logging in to SDS in an inappropriate environment or place.	ESRC/ONS/UK Data Service	SDS Agreement Violation of Statutory Law (Criminal Offence) / Violation of Statutory Law (Criminal Offence) for ONS data
Failure to report a disclosure	*Expected Penalty for HE researchers* a) Permanent suspension (individual); AND b) 1 year suspension (institution) AND c) 2 year sanction from ESRC funding (individual) AND d) 1 year sanction from ESRC funding (institution) *Penalty for non-HE researchers* a) Permanent suspension (individual); AND b) 5 year sanction from ESRC funding (individual)	An example includes where there has been an unintentional disclosure and the researcher has not informed the UK Data Service.	ESRC/ONS/UK Data Service	Licence violation (Civil Offence) / Violation of Statutory Law (Criminal Offence) for ONS data
Attempt to identify respondents	*Expected Penalty for HE researchers* a) Permanent suspension from all ESRC data services (individual); AND b) 1 year suspension from all ESRC data services (institution) AND c) permanent sanction from ESRC funding (individual) AND d) 5 year sanction from ESRC funding (institution) *Expected Penalty for non-HE researchers* a) Permanent suspension from all ESRC data services (individual); AND b) Permanent sanction from ESRC funding (individual) For ONS Approved Researchers attempting to re-identify respondents is a criminal offence,	This is where a researcher attempts to identify an individual, household or business in the data.	ESRC/ONS/UK Data Service	Violation of Statutory Law (Criminal Offence) / Violation of Statutory Law (Criminal Offence) for ONS data

	and breaches may be subject to prosecution at the discretion of ONS.			
Making disclosive data available to others	*Expected Penalty for HE researchers* a) Permanent suspension from all ESRC data services (individual); AND b) 5 year suspension from all ESRC data services (institution) AND c) permanent sanction from ESRC funding (individual) AND d) 5 year sanction from ESRC funding (institution) *Expected Penalty for non-HE researchers* a) Permanent suspension from all ESRC data services (individual); AND b) Permanent sanction from ESRC funding (individual) Making disclosive ONS data available to others is a criminal offence and breaches may be subject to prosecution at the discretion of ONS. Identifying a ONS respondent and providing that detail to another party for personal gain is a serious criminal offence in the Statistics and Registration Service Act, with potentially a 2 year jail term, a £2000 fine, and a criminal record.) Making non-ONS disclosive data available to others is a criminal offence and may be subject to prosecution at the discretion of the ESRC and the data depositor.		ESRC/ONS/UK Data Service	Violation of Statutory Law (Criminal Offence) / Violation of Statutory Law (Criminal Offence) for ONS data