Implementation of the Data Seal of Approval

The Data Seal of Approval board hereby confirms that the Trusted Digital repository UK Data Archive complies with the guidelines version 2014-2017 set by the Data Seal of Approval Board.
The afore-mentioned repository has therefore acquired the Data Seal of Approval of 2013 on June 9, 2015.

The Trusted Digital repository is allowed to place an image of the Data Seal of Approval logo corresponding to the guidelines version date on their website. This image must link to this file which is hosted on the Data Seal of Approval website.

Yours sincerely,

The Data Seal of Approval Board

Assessment Information

Guidelines Version: 2014-2017 | July 19, 2013
Guidelines Information Booklet: DSA-booklet_2014-2017.pdf
All Guidelines Documentation: Documentation

Repository: UK Data Archive
Seal Acquiry Date: Jun. 09, 2015

For the latest version of the awarded DSA   http://assessment.datasealofapproval.org/seals/
for this repository please visit our website:

Previously Acquired Seals: Seal date: March 8, 2011
                                  Guidelines version: 2010 | June 1, 2010

This repository is owned by: **UK Data Archive**
                                  University of Essex
                                  Wivenhoe Park

                                  CO4 3SQ Colchester
                                  Essex
                                  U.K.

                                  T 01206873162
                                  E herve@essex.ac.uk
                                  W http://www.data-archive.ac.uk/

Assessment

0. Repository Context

Applicant Entry

Self-assessment statement:

The UK Data Archive

The UK Data Archive (UKDA) is a centre of expertise in data acquisition, preservation, dissemination and promotion and is curator of the largest collection of digital data in the social sciences in the UK. The UK Data Archive is a department within the University of Essex, and thus it is the University which is the legal entity. The UKDA was founded in 1967, and it currently houses several thousand datasets of interest to a wide range of researchers and provides resource discovery and support for secondary use of quantitative and qualitative data in research, learning and teaching.

Like most modern repositories/data management services the UK Data Archive exists within a complex framework of stakeholders. But equally we understand that the boundary on any Trusted Digital Repository (TDR) standard, including the DSA must be well-defined to ensure that the wider community is clear on what is included in the certification.

This application for the DSA is limited to the UK Data Archive (**W1**) based at the University of Essex, UK, as trusted digital repository, and covers the 'main collection'. Exclusions do not detract from the quality, trustworthiness and value of the functions and services not covered, they are a practical decision based on the following criteria:
*The UK Data Archive at Essex University is a clearly defined online presence (as required by the DSA)
*The UK Data Archive has information and premises security certified to ISO27000 (**R1**)

This has lead to the decision that the following are not included in this application, though relevant processes may be mentioned to place them in context:
*Collections ingested off-site
*Self-Archiving services with lower curation levels, file format and metadata requirements
*Collections for which we do not hold a specific long term digital preservation remit
*Virtual Collections visible in the catalogue but not accessible via our systems

The UKDA is a partner organisation in the UK Data Service, funded by the Economic and Social Research Council (ESRC), to provide research data infrastructure in the UK. The UK Data Service is the nominated national Service Provider to CESSDA (Consortium of European Social Science Data Archives). A proportion of the

self-assessment statements and evidence links refer to UK Data Service web sites and branded documentation. In all cases where such evidence is presented it is subject to UK Data Archive standards in addition to UK Data Service standards including approval by a Policy Group, documentation approval and management via a Governance Oversight Committee and documentation approval and management and information and premises security management through a Information Security Management Group (a requirement for certification against ISO27000).

The catalogue containing in-scope UK Data Archive resources is currently available on the UK Data Service domain (**W2**). High quality data collections and catalogue records available via the Discover system but excluded from this application are Administrative Data Service (catalogue record only, no data held), ReShare (self-archive repository with separate deposit criteria), International Data (processed by colleagues at JISC Manchester) and Census data collections (processed by colleagues at JISC Manchester, Cathie Marsh and UCL).

Standard and classifications in use include the following: Data Documentation Initiative), ELSST (European Language Social Science Thesaurus), ISO27000 for Information Security, OAIS (Open Archival Information System) reference model. We acquire high quality data from the academic, public, and commercial sectors, providing continuous access to these data while also supporting existing and emerging forms of data and communities of data users.

The managed 'unit' of information at the data archive is termed a 'data collection'. External roles are generally referred to as 'depositors' (not necessarily the data producer, which may refer to the pre-deposit custodian and to those with the rights to negotiate licences and grant conditional access provisions) and 'user' or 'end users'. Depositors may be characterised as 'new depositors', 'regular depositors' or as 'ESRC Award Holders'. Those holding awards from the Economic and Social Research Council deposit their data into the ReShare self-deposit system within three months of the end of their grant.

Repository Process Overview

D1: Repository Workflow Overview: Data and
Metadata http://www.data-archive.ac.uk/media/3721/D1-HLH-RepositoryProcessOverview_01_00.png

An overview of workflow and data flows with some designated as 'core' which map to the OAIS and the data lifecycle for the purposes of this self-assessment

D2: Business Process Overview:
Repository http://www.data-archive.ac.uk/media/3722/D2-HLH-PresPlan-RepositoryProcesses_01_00-Overview.png

An overview of business processes, linked business processes for items with a dark blue shadow are included below. More detailled process descriptions exist but are not included as part of this self-assessment statement for reasons of brevity.

Pre-Ingest

D3: Business Process Overview:
Pre-Ingest http://www.data-archive.ac.uk/media/3722/D2-HLH-PresPlan-RepositoryProcesses_01_00-Overview.png

This stage from the point of first contact with a potential depositor to the receipt of an approved deposit for ingest is characterised as 'pre-Ingest', the 'preliminary phase' of the producer-archive interface in PAIMAS (http://public.ccsds.org/publications/archive/651x0m1.pdf) terms.

Ingest

D4: Business Process Overview:
Ingest http://www.data-archive.ac.uk/media/3724/D4-HLH-PresPlan-RepositoryProcesses_01_00-Ingest.png

Ingest procedures are undertaken from the point of internal custody transfer from pre-ingest to the point of custody transfer to Archival Storage (AIP) and Access (DIP)

Access

D5: Business Process Overview:
Access http://www.data-archive.ac.uk/media/3725/D5-HLH-PresPlan-RepositoryProcesses_01_00-AccessOverview.png

Access management from the user perspective.

Archival Storage

D6: Archival Storage: Multi-copy
Resilience http://www.data-archive.ac.uk/media/3726/D6-HLH-ArchivalStorage-MultiCopyResilience_02_00.png

An overview of the multi-copy resiliency model for Archival Storage.

Outsourcing

None of the functions subject to this DSA Self-Assessment are outsourced though strong partnerships exist including with the UK Data Service and the University of Essex these are explained above.

Evidence

*Evidence files are provided at a single location for consistency and to ensure availability. Evidence files are marked as F or D for diagrams

*Evidence available as web pages are linked to. Evidence on the web is marked with a W

*Information included for reference or context rather than evidence is marked as R

Each is designated an ID (F1, D1, W1, R1 etc) to help manage them over time.

References to web pages at the UK Data Archive, or provided to Data Depositors and Users via the UK Data Service website are subject to change over time. Information related to any broken links during the lifetime of the Seal will be provided at the standard evidence location

W1: UK Data Archive Website http://www.data-archive.ac.uk/

W2: Resource Discovery via UK Data Service http://discover.ukdataservice.ac.uk/

R1: ISO27001 http://www.iso.org/iso/catalogue_detail?csnumber=63411

D1: Repository Workflow Overview: Data and Metadata http://www.data-archive.ac.uk/media/3721/D1-HLH-RepositoryProcessOverview_01_00.png
D2: Business Process Overview: Repository http://www.data-archive.ac.uk/media/3722/D2-HLH-PresPlan-RepositoryProcesses_01_00-Overview.png

D3: Business Process Overview: Pre-Ingest http://www.data-archive.ac.uk/media/3722/D2-HLH-PresPlan-RepositoryProcesses_01_00-Overview.png

D4: Business Process Overview: Ingest http://www.data-archive.ac.uk/media/3724/D4-HLH-PresPlan-RepositoryProcesses_01_00-Ingest.png

D5: Business Process Overview: Access http://www.data-archive.ac.uk/media/3725/D5-HLH-PresPlan-RepositoryProcesses_01_00-AccessOverview.png

D6: Archival Storage: Multi-copy Resilience http://www.data-archive.ac.uk/media/3726/D6-HLH-ArchivalStorage-MultiCopyResilience_02_00.png

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

This context statement is excellent. It sets the stage for the assessment and indicates what is in and out of scope. Further, it positions the archive in the OAIS context.

1. The data producer deposits the data in a data repository with sufficient information for others to assess the quality of the data, and compliance with disciplinary and ethical norms.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

3. In progress: We are in the implementation phase.

Self-assessment statement:

For data to be accepted into the collection sufficient information should be provided at the time of deposit for others to asses the quality of the data; otherwise we work with the depositor to enrich deposited metadata to meet our standards. All information deposited is retained. Information relevant to the use of data, including evaluation of quality, is made available in the Dissemination Information Package (OAIS: DIP) provided to the data user.

Some quality and ethical issues are somewhat sector-specific, e,g, provision of explicit guidance for depositing survey data suitable for sharing (**F1**)

Our guidance explicitly states that any data deposited should be free from any legal or ethical issues that might limit the sharing of data. The terms and conditions of deposit place responsibilities upon the depositor (**W3**) including:
* guarantees that nothing in the data collection is illegal,including breaches of privacy or data protection laws
* assurances that they have obtained the agreement of all parties who may have an interest in the data collection
* that copyright interest has been included in the schedule to the Licence Agreement.

Comprehensive advice is provided for all stages of the data-lifecycle and on a variety of relevant issues:

*research data management training is offered including in-person events and webinars. Bespoke training is available on request and extensive supporting materials are available online to researchers planning data creation with a view to creating shareable outputs.

*guidance on creating, sharing, costing and data management (**W4**)

*Content covering ethical and legal issues, consent, anonymisation and access control (**W5**)

*Specific guidance is provided upon legal and ethical obligations in research including data protection, freedom of information, human rights, research ethics approval and the Statistics Act 2007 (**W6**)

We proactively acquire data that are suitable for use in research and teaching and with the scope of the Collections Development Policy (**F2**) so while 'proof of identify' is not practical we have close relationships with main collection depositors, often over long periods of time especially in the common case of depositors which are government departments or which have been funded through the Economic and Social Research Council (http://www.esrc.ac.uk/). ESRC-funded research is subject to specific conditions and deposits are linked to unique funding identifiers.

Guidance materials on submission to the repository are provided (**W7**) including who can deposit (government departments, researchers and research institutions, public organisations and companies) and how to undertake the process.

A New Depositor Data Offer Form (**F3**) collates details relating to the depositor, their organisation, and funding information as well as title, abstract and file descriptions for the data offered.

References and links to publications based on the data are requested as is information related to consent (for research involving individuals, households or organisations), anonymisation and confidentiality.

Offers of data are evaluated against appraisal criteria (**F4**) which includes the statement "to provide researchers with access to original research that allows checks for consistency, validation of sources and validation and replication of research outputs, both published and unpublished". Appraisal criteria include several levels of curation (Long-term curation, short term management, delivery only, discovery only, preservation only) which are considered during several stages of evaluation (strategic high-level value, user need and analytic value, and potential usability and accessibility).

The Data Deposit Form (**F5**) includes details about the methodology employed including observation units,

method of data collection and sampling procedures. Details of any weighting applied is also requested.

Depositors are expected to undertake an ethical review to ensure that there is no potential for risk of harm to any participants in making data available to third parties. The ESRC's Research Ethics Framework (REF) (**R2**) provides a framework which we and researchers work within.

Our compliance level remains at "3. In progress: We are in the implementation phase" rather than level 4 because we are working to develop approaches to new and novel forms of data including 'big' and 'administrative' data.

Evidence:

****

W1 UK Data Archive Website http://www.data-archive.ac.uk/
W2 Resource Discovery via UK Data Service http://discover.ukdataservice.ac.uk/
R1 ISO27001 http://www.iso.org/iso/catalogue_detail?csnumber=63411
F1 Depositing Sharable Survey Data: http://ukdataservice.ac.uk/media/440320/depositsurvey.pdf
W3 Data Deposit http://www.data-archive.ac.uk/conditions/data-deposit)
W4 Guidance on Data Management http://www.data-archive.ac.uk/create-manage
W5 Consent and Ethics Guidance http://www.data-archive.ac.uk/create-manage/consent-ethics
W6 Ethical and Legal Guidance http://ukdataservice.ac.uk/manage-data/legal-ethical.aspx
F2 Collections Development
Policy http://ukdataservice.ac.uk/media/398725/cd227-collectionsdevelopmentpolicy.pdf
W7 Guidance on Submission to the Repository http://www.data-archive.ac.uk/deposit
F3 New Depositor Data Offer Form http://www.ukdataservice.ac.uk/media/455252/data_offer_form.docx
F4 Collections Development and
Appraisal http://ukdataservice.ac.uk/media/455175/cd234-collections-appraisal.pdf
F5 Data Deposit Form http://ukdataservice.ac.uk/media/158537/data_deposit_form.docx
R2 ESRC Research Ethics
Framework http://www.esrc.ac.uk/_images/framework-for-research-ethics_tcm8-33470.pdf

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

2. The data producer provides the data in formats recommended by the data repository.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

All file formats are potentially at risk from the obsolescence of the hardware and software environments upon which their rendering depends. Initial conversion to acceptable preservation and dissemination formats is best undertaken by researchers familiar with the original data. We require deposit of data in formats suitable for long term preservation or those which can be converted to such formats. A format list is provided (**W08**). Forward migration of 'at risk' formats is undertaken as needed and Archive staff have a 'tech watch' remit which includes file format risk. Data are delivered to users in current, common data formats which are suitable for our designated community.

Collections appraisal criteria for not accepting data collections include "Old/unreadable formats that are difficult to convert or make usable, or impossible to recover" (**F04**).

A processing standard (**F18**) is assigned to each main collection deposit depending on the nature and condition of the data, the quantity and complexity of the documentation, the estimated level of use and whether or not the data collection is to be made available through online browsing tools (**W10**).

If data are deposited in non-preferred formats we work with data producers and a range of software tools to enable us to convert data to an acceptable format where possible and if not, to ensure that guidance is provided for users to enable them to find tools to use the data. Only Quantitative processing standard C has a reduced file format requirement and this is only used for those studies where the materials are in very poor condition with little improvement possible, or are in a software-dependent format with no alternatives available.

Internal procedures including quality control during the pre-ingest and ingest process ensure formats are compliant with our recommendation

Evidence:

****

W08 Format List http://ukdataservice.ac.uk/manage-data/format/recommended-formats.aspx

F04 Collections Development and
Appraisal http://ukdataservice.ac.uk/media/455175/cd234-collections-appraisal.pdf

F18 Data Processing
Standards http://www.data-archive.ac.uk/media/54782/ukda079-ds-dataprocessingstandards.pdf

W10 Online Browsing Tools http://www.data-archive.ac.uk/find/online-data-browsing

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

3. The data producer provides the data together with the metadata requested by the data repository.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

As well as "sufficient information for others to assess the quality of the data, and compliance with disciplinary and ethical norms" (Guideline 1) the metadata associated with a data collection must support an understanding of its provenance, and be sufficient to apply appropriate access criteria, support resource discovery and be sufficient to guide end users undertaking secondary analysis.

A 'new depositor' Data Offer Form (**F3)**) collates details relating to the depositor, their organisation, and funding information ass well as basic title, abstract and file descriptions for the data offered. References and links to publications based on the data are requested as is information related to consent (for research involving individuals, households or organisations), anonymisation and confidentiality. The Data Deposit Form (**F5**) includes details about the methodology employed including observation units, method of data collection and sampling procedures. Details of any weighting applied is also requested. A file manifest is also necessary to cross-check against the submitted data collection.

We recognise that both documentation (relatively unstructured supporting materials) and metadata (structured against some recognised standard) are important to the administration, understanding and use of data collections. The Data Documentation Initiative (DDI) is the Social Science domain standard. Metadata requested is sufficient to complete a DDI version 2.5 catalogue record to support resource description and discovery which is also mapped to Dublin Core.

Controlled vocabularies are taken from domain standards wherever possible and we use the Humanities and Social Sciences Electronic Thesaurus (HASSET), the English language portion of the European Language Social Science Thesaurus (ELSST) (**W11**)

Metadata quality control is undertaken when data is offered and when deposited. Metadata must be complete and sufficient for all purposes, including access management, use and preservation, before the data collection can be released. Guidance for documentation of data is provided (**W12**) and detailed catalogue procedures and guidelines

published (**F6**)

Evidence:

****

F3 New Depositor Data Offer Form http://www.ukdataservice.ac.uk/media/455252/data_offer_form.docx
F5 Data Deposit Form http://ukdataservice.ac.uk/media/158537/data_deposit_form.docx
W11 European Language Social Science Thesaurus (ELSST) http://elsst.ukdataservice.ac.uk/
W12 Guidance for Documentation http://ukdataservice.ac.uk/manage-data/document.aspx
F6 Catalogue Procedures &
Guidelines http://data-archive.ac.uk/media/401477/ukda035-cataloguingproceduresandguidelines.pdf

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

4. The data repository has an explicit mission in the area of digital archiving and promulgates it.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

Our mission statement which is included in our Strategic Plan (**F7**), released under the authority of the Director and with the support of our funders and the University of Essex, states that the organisation is:
"a leading centre of expertise in data archiving in the UK. It holds the largest collection of digital data in the social sciences and humanities in the UK and makes them available to the higher and further education sector and beyond for research, teaching and learning. Its mission is to maintain its leading role by continuously improving the quality and breadth of its data products and services in response to user needs and technological changes. To this end it collaborates with national and international organisations to develop new data standards and tools. It also aims to build bridges between data creators and data users across different sectors and disciplines."

We recognise that the preservation/continued access mission is implicit within this statement and intend to make it explicit in future iterations of the strategic plan/mission statement. The Strategic Plan includes a section on 'Selection, Acquisition, Ingest and Preservation' and Strategic Goals include 'promote best practice in data curation through collaboration', 'improve access to and use of data', 'raise standards in data management and security', 'drive archival innovation' and 'demonstrate excellence in accountability and operations'.

The Strategic Plan specifically references the Data Seal of Approval and related trust standards, stating that the organisation will: " demonstrate its commitment to international standards. It shall champion the Data Seal of Approval as starting point for trusted digital data repositories, and will work towards conformity and compliance to other relevant standards in the digital curation arena."

The Archive's mission and strategic goals are implemented through participation as partners in a variety of projects, through the provision of training and supporting materials to data producers and data consumers and through cooperation with other Archives, including but not limited to the Consortium of European Social Science Data Archives (CESSDA).

The Archive implements its preservation mission through a Preservation Policy (**F8**). We follow a policy of active preservation to ensure the authenticity, reliability and logical integrity of all resources entrusted to our care while providing usable versions for research, teaching or learning, in perpetuity.

Our Business Continuity Incident Management Procedures (**CD091**) (not public, available to reviewer on request) developed in line with certification against ISO27000 for Information Security includes the following reference to succession planning:

"In the event that the Archive has to permanently cease operation because of loss of funding a formal succession plan would be prepared. As the loss of funding would be likely to involve at least eighteen months' notice this would allow sufficient time to establish a Succession Task Team to prepare a plan at least three months before funding ceased. The plan would cover succession, software and records escrow and negotiation of rights transfer. The University would be involved in any closure of the Archive."

We undertake significant outreach activities related to data management and continued access including participation in the Digital Preservation Coalition (DPC) http://www.dpconline.org.

Evidence:

****

F7 Strategic Plan http://www.data-archive.ac.uk/media/196518/ukda-strategicplan20102015full.pdf
F8 Preservation Policy http://www.data-archive.ac.uk/media/54776/ukda062-dps-preservationpolicy.pdf
F9 Business Continuity Incident Management Procedures (CD091) not public, available to reviewer on request

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

It is good that the repository is thinking about business continuity and succession planning. In the future it would be good to explore partnerships with peer institutions that would explicitly cover succession planning for digital assets.

5. The data repository uses due diligence to ensure compliance with legal regulations and contracts including, when applicable, regulations governing the protection of human subjects.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

All contracts with third parties are technically with the University of Essex (a limited company) as the legal entity. Our Preservation Policy (**F8**) defines the legal and regulatory framework.

The relationship with the depositor of a data collection is based on:

*a legally-binding deposit agreement and licence (known as the Licence Agreement) which confirms the rights and obligations of both parties and offers an opportunity for depositors to specify the conditions under which access may be given to third parties;
*an assertion of copyright and intellectual property rights to ensure that the data creator/depositor has cleared all necessary permissions;
*where necessary, negotiations for licence agreements with third parties to enable the us explicitly to distribute the material to particular user communities.

We will not ingest materials that have unclear ownership or unresolved rights issues.

In preserving its collections, we follow:

*English or UK law for commercial agreements and contract law

*Copyright, Design and Patents Act, 1988 and amendments to this Act;

*Data Protection Act, 1998;

*Statistics and Registration Services Act, 2007

*Freedom of Information Act, 2000;

*EU Copyright Directive, 2001;

*Environmental Information Regulations, 2004;

We are certificated to BS ISO/IEC 27000 (**R1**) and follow the Cross Government Actions: Mandatory Minimum Measures (**R3**).
Depositors must review ethical issues relating to data collections they wish to deposit including those surrounding the potential for risk of harm to any participants in making data available to third parties.
The ESRC's Research Ethics Framework (**R2**) provides guidance to both the Archive and to its researchers.

While it is the responsibility of depositors to ensure data with a disclosure risk are not unintentionally deposited staff are trained in the handling of data with disclosure risk. Data with an unintended disclosure risk may be identified during quality assurance at the pre-ingest or ingest stage and rejected. Data with a known disclosure risk are subject to special procedures, handling, storage and access conditions and methods. Data are protectively marked and handled according to their level of detail. Data destined for Secure Lab access are stored and processed on separate secure servers.

Standard model deposit licences are in use (**F9**), deposits undertaken from the UK Office of National Statistics

ONS are governed by a mutually agreed concordat.

Standard model end user licences are in use. Since 2008, the UK Data Archive promotes 'open data' with the use of a de facto access condition of open to all comers, for all uses but terms and conditions of access (**W13**) to some data collections are governed via a standard end user licence (EUL). If additional conditions of use exist these are agreed to online via a special conditions statement or, in cases where additional information is needed and/or additional permission must be sought a special licence is issued. In cases where data are deemed too confidential or sensitive to be released (E.g disclosure risk) via normal access channels secure access approaches employed (appropriately approved and trained researchers may use collections via secure remote connections or in a safe room).

Breaches procedures (controlled documents **142** and **246,** not public, available to reviewers upon request) are in place if terms and conditions of use are violated.

All Archive staff are required to sign a non-disclosure agreement (**F13**). The Archive follows its own advice relating to regulations dealing with the protection of human subjects

(**W5**)

Evidence:

****

F8 Preservation Policy http://www.data-archive.ac.uk/media/54776/ukda062-dps-preservationpolicy.pdf
R1 ISO27000 http://www.iso.org/iso/catalogue_detail?csnumber=63411
R3 Cross Government Mandatory Minimum
Measures https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60968/cross-gov-actions.pdf
R2 ESRC Research Ethics
Framework http://www.esrc.ac.uk/_images/framework-for-research-ethics_tcm8-33470.pdf
F9 Deposit Licence Form http://ukdataservice.ac.uk/media/28102/licenceform.pdf
W13 Terms and Conditions of Access http://www.data-archive.ac.uk/conditions/data-access
F11 Licence Compliance Policy
(CD142) http://ukdataservice.ac.uk/media/311391/CD142-LicenceCompliancePolicy.pdf

F12 Managing Licence Compliance (CD246) not public, available to reviewers upon request
F13 Non-Disclosure Agreement
W5 Consent and Ethics Guidance http://www.data-archive.ac.uk/create-manage/consent-ethics

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

6. The data repository applies documented processes and procedures for managing data storage.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

We undertake data storage against documented processes and including procedures in line with ISO27000 Information Security (**R01**) standards.

The Archive provides guidance on the transfer of data to initial storage locations, ideally via the ZendTo product, and on encryption of data during that process (**W14**)

Separate network locations are designated for pre-ingest and ingest teams to hold deposited data and versions of files being curated to create archival (AIP) and dissemination information packages (DIP) from submission information packages (SIP). The team which manage end user Access to resources also have a dedicated workspace. Each network location is accessible only to relevant security group (Microsoft Active Directory) members.

Formal archival storage (OAIS) practices are implemented from the point of custody transfer from the Ingest team. The notification and details of the transfer request and response are handled through a help desk system. Once an AIP (including embedded SIP and DIP) is complete a transfer request is made and completed by creating a new, or updating an existing data collection. The strategy for multiple copies/backups is outlined in the Preservation Policy (**F08**) and implemented for all data collections for which we have long term digital preservation responsibility.

The transfer creates a copy (copy 1) of the AIP on the main preservation server and onto a front end server (copy 2) visible to (but not editable by) the Ingest team for final QA of the transfer process in the main server space. Copies 3 and 4 are made to an additional on-site server location and a near-site server respectively. A 5th offline copy is made to disc drive and stored in a tape safe and a 6th copy is maintained off site.

The Archival Storage team undertake the 'manage storage hierarchy' function (OAIS) including storage management policies. It monitors error logs to ensure AIP are not corrupted during transfers and maintains operational statistics such as media inventories, available storage capacity in the various storage tiers and usage statistics.

All main collection items receive the same level of security with secure access data being managed by a CITRIX system for storage and access.

Secure access data is on a network segregated from the main collection. Users are required to undergo additional training and security checks before access is granted through a heavily restricted Citrix environment. This Citrix environment has been configured to prevent unauthorised data removal.

The 'replace media function' (OAIS) refers to periodic media 'refreshment', 'replication', 'repackaging' (OAIS) which is undertaken a maximum of every 3 to 5 years or earlier if errors are detected.
 S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) monitoring systems are in place.

Note: under OAIS "complex 'Repackaging' and all 'Transformation' are performed under Administration supervision by the Archival Information Update function to ensure information preservation". At the Archive such file format transformations and other updates (whether to meet user needs for differing file formats or to move away from 'at risk' formats) are undertaken through 'on demand processing' by the Ingest team.

The overall integrity of the multiple copies (the Error Checking function under OAIS) is ensured through the cross-checking of checksums periodically and after any data transfer event. Any errors detected result in a replacement from an error-free copy of the data.

In the event of the need for disaster recovery (OAIS) the duplicate copies held by Archival Storage would be used.

Evidence:

****

W14 Encrytion for transfer http://www.data-archive.ac.uk/create-manage/storage/encrypt
R01 ISO27000 http://www.iso.org/iso/catalogue_detail?csnumber=63411
F08 Preservation Policy http://www.data-archive.ac.uk/media/54776/ukda062-dps-preservationpolicy.pdf

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

7. The data repository has a plan for long-term preservation of its digital assets.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

Our preservation strategy (**F08**) is based upon open and available file formats, data migration and media refreshment.

Preservation decisions are made within the context of our Collections Development Policy (**F02**), balancing the constraints of cost, scholarly and historical value, and user accessibility alongside the requirements of levels of authenticity and legal admissibility. Different ingest processes may be required for material with different levels of quality and significance. Data collections are assigned an ingest activity level as outlined in Collections Development Selection and Appraisal Criteria (**F04**).

The preservation strategy is predicated on two basic principles:

*first, that digital storage media are inherently untrustworthy unless stored appropriately;

*second, that all file formats and physical storage media will ultimately become obsolete.

Therefore, the environmental parameters which control the storage media are tightly controlled to reduce the vulnerability of these media. Additionally, the strategy to reduce the risk of obsolescence is based on storing multiple copies on different storage media (see multi-copy resilience information under guideline 6: Data Storage Processes). These are reviewed regularly and data are copied onto new media when appropriate. A similar strategy is employed to deal with the obsolescence of file formats. Appropriate information-rich preservation formats have been identified and are used in conjunction with formal documentation procedures. These formats are chosen with specific reference to the 'data types' under consideration (**W08**). This list is reviewed on an annual basis to assess ongoing file format risk.

Deposited files must either be in an acceptable file format or be capable of transformation to an acceptable format.

The majority of quantitative microdata files are deposited in SPSS format which is also the most popular dissemination format. Processing a quantitative study therefore typically entails converting the data into SPSS .sav format where appropriate and creating dissemination and preservation formats (usually SPSS, Stata and tab-delimited text).

Most qualitative data collections currently acquired take the form of individual interview, or focus group, transcripts received in Word or Rich Text Format (RTF) format, and are made available as RTF. In rare cases where qualitative material is provided as Tagged Information Format File (TIFF) files (usually old collections where paper documents have been scanned), the TIFF files are grouped together as Adobe Portable Document Format (PDF) files.

The ingest function transforms all elements of the deposited files into a valid preservation format for the specified data type. File format transformations after data collections have moved to archival storage may be triggered based on an identified risk or by request from users for alternate dissemination formats for use. When new formats are created from data files either through migration into new file formats or through creating new file formats for dissemination, the previous files are retained alongside the original deposits.

The main steps for providing long-term preservation of digital research data are contained in our preservation policy and detailed guidance is provided in ingest procedures (**F17**)

Evidence:

****

F02 Collections Development
Policy http://ukdataservice.ac.uk/media/398725/cd227-collectionsdevelopmentpolicy.pdf
F04 Collections Development and
Appraisal http://ukdataservice.ac.uk/media/455175/cd234-collections-appraisal.pdf
W08 Format List http://ukdataservice.ac.uk/manage-data/format/recommended-formats.aspx
F17 Ingest processing quick
reference http://www.data-archive.ac.uk/media/54764/ukda080-ds-processingquickreference.pdf

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

8. Archiving takes place according to explicit work flows across the data life cycle.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

3. In progress: We are in the implementation phase.

Self-assessment statement:

We are committed to using diagrammatic and documented workflow descriptions to ensure consistent management of data collections and to ensure managed change to business processes. The entire archival process from pre-ingest through to access is predetermined based on data collection types, file formats and access criteria.

Procedures are in place to support pre-ingest (from first point of contact with a potential depositor to the point of deposit), ingest, access, archival storage and preservation planning. These sections of the organisation undertake the relevant OAIS administration functions and ensure data management.

All data acquisitions are in line with selection and appraisal criteria in our collections development policy (**F02**). Data producers are offered full information on the processes undertaken on data deposited (**W16**). Pre-ingest procedures (**F14**) not currently public, available to reviewer upon request) govern the deposit process and associated quality checks.

File format transformations on ingest are based on approved file formats which are evaluated based on risk of obsolescence (for preservation formats) and utility to the designated community of users (for dissemination formats). Data collections are primarily quantitative and qualitative and these have documented procedures for curation throughout including file format transformations, quality assurance and appropriate supporting metadata and documentation. Guarding the privacy of subjects is important for data collections designated as potentially disclosive and additional procedures exist.

Recruitment and selection procedures ensure that staff have appropriate skills at the point they are hired. Ongoing training requirements are identified through appraisal and personal development schemes.

Lifecycle and business process diagrams are in place to support the specification and redevelopment of internally developed software for data and metadata management and these will be integrated into change management procedures (alongside change management for metadata and controlled vocabularies) when that system is released.

Evidence:

****

F02 Collections Development
Policy http://ukdataservice.ac.uk/media/398725/cd227-collectionsdevelopmentpolicy.pdf
W16 Curation process http://www.data-archive.ac.uk/curate/process
F14 Pre-Ingest Procedures not currently public, available to reviewer upon request
F17 Ingest processing quick
reference http://www.data-archive.ac.uk/media/54764/ukda080-ds-processingquickreference.pdf
F15 Qualitative Processing
Procedures http://www.data-archive.ac.uk/media/54767/ukda093-ds-qualitativeprocessingprocedures.pdf

F16 Quantitative Processing
Procedures http://www.data-archive.ac.uk/media/54770/ukda081-ds-quantitativedataprocessingprocedures.pdf
F02 Collections Development
Policy http://ukdataservice.ac.uk/media/398725/cd227-collectionsdevelopmentpolicy.pdf

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

9. The data repository assumes responsibility from the data producers for access and availability of the digital objects.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

We take explicit responsibility for access to and availability of all data collections selected for long term curation at the point that a data collection is released but never assume sole responsibility for access to and availability of any
data. Contractually, data producers are allowed to make their own data available in any means that they wish so responsibility may be shared with the data producer.

This responsibility is governed by a standard deposit licence(**F10**). Access is managed based on criteria agreed at the time of deposit as 'open' (through open government licence, creative commons licence or equivalent open licence), 'safeguarded' (for data with some residual disclosure risk but containing no Personal Data nor Personal Information) or 'Controlled Access' (for Personal Information, Personal Data or data that are particularly sensitive, commercially or otherwise.

Licences are agreed with the University of Essex as the legal entity to hold, make copies of, and provide access to the Data Collection, in accordance with the specified access condition. The licence is non-exclusive; this means that the data owner(s) can deposit and/or make available their data collection elsewhere. Copyright in the original data remains with the data owner(s) and is not transferred when data are deposited.

It remains within the rights of the depositor to withdraw the data collection so there is little practical issue with the enforcement of this licence from our perspective.

As part of certification to ISO27000 for Information Security (R01) a Business Continuity Incident Management Procedure CD091 (**F09**) which covers provision of access to data and a worst case scenario statement on succession planning as follows

"In the event that the Archive has to permanently cease operation because of loss of funding a formal succession plan would be prepared. As the loss of funding would be likely to involve at least eighteen months' notice this would allow sufficient time to establish a Succession Task Team to prepare a plan at least three months before funding ceased. The plan would cover succession, software and records escrow and negotiation of rights transfer. The University would be involved in any closure of the Archive."

Evidence:

****

F10 Deposit Licence Form http://ukdataservice.ac.uk/media/28102/licenceform.pdf
R01 ISO27000 http://www.iso.org/iso/catalogue_detail?csnumber=63411
F09 Business Continuity Incident Management Procedures (CD091) not public, available to reviewers upon request

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

10. The data repository enables the users to discover and use the data and refer to them in a persistent way.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

Clear standards for metadata upon deposit are specified. Metadata and documentation to support discovery and use are created during ingest are defined in Cataloguing Procedures and Guidelines (**F06**).

All data collections for which this DSA application applies are searchable (**W02**)and an OAI-PMH harvester for DDI2.5 and Dublin Core metadata is available (**W17**). All searches are at data collection level. The Nesstar (**W18**) product contains a subset of quantitative data collections documented to and searchable at variable level.

Access to resources depends on their access criteria which may be open, safeguarded (subject to a standard end user licence for registered users and potentially to additional conditions, depositor permission etc) or controlled (users must be registered users who have been approved by a Data Access Committee)

Research data is currently available in formats which the data consumers request or use frequently. For statistical data, files are currently provided in SPSS, Stata and text formats. Our access and user support functions maintain close relationships with our designated community and new file formats for use are created when demand arises, users may also request data in alternate formats. In both cases these transformations may be undertaken by the Ingest team.

All data collections are assigned a digital object identifier (DOI) minted through the DataCite service (**R04**). Major changes to collections are supported by a new DOI. All changes to data collections are supported by a change log on a DOI 'jump' page in addition to the more detailled 'read' files which are included in data downloads. Each data collection contains specific citation instructions which include the DOI.

Evidence:

****

F06 Catalogue Procedures &
Guidelines http://data-archive.ac.uk/media/401477/ukda035-cataloguingproceduresandguidelines.pdf)
W17 OAI-PMH http://oai.ukdataservice.ac.uk/oai
W18 NESSTAR http://nesstar.ukdataservice.ac.uk/webview
R04 DataCite https://www.datacite.org/

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

11. The data repository ensures the integrity of the digital objects and the metadata.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

3. In progress: We are in the implementation phase.

Self-assessment statement:

In OAIS the data integrity service "ensures data is not altered or destroyed in an unauthorized manner"

Our activities are based on a pragmatic interpretation of integrity, full copies of original submission information package (SIP) are retained. The data collections which are accessed by users are complete, but they are not unaltered from the originally deposited data collection. New versions are made to support access and digital preservation, but the changes which have been made from the SIP are documented and released with the data collection (see Guideline 12: Authenticity)

As a repository with close contact with many depositors there may be several interactions and partial deposits before the existence of a formal SIP is declared. Our role in quality assurance and enrichment implies that Ingest team members must have free access to copies of deposits for conversion into DIP and AIP including format conversion, metadata enrichment and creation and review of supporting contextual documentation. This, and the manual file transformation processes mean that pre- and post-amendment checksums cannot be reasonably created for each pre-Ingest and Ingest team action but all actions are fully documented.

When a new or amended deposit moves from the Ingest to the Archival Storage team a checksum (MD5) is generated for each file within the Archival Information Package (AIP). These checksums are cross-checked periodically and during copy actions within archival storage (see guideline 6: Data Storage Processes).

Dissemination Information Packages (DIP) have a checksum (MD5) generated against all of the files, this checksum is appended to the overall zip file name and can be used to validate the download.

Each new deposit is treated as a new 'version' of the data collection and on transfer to archival storage this replaces the previous version. All previous releases are maintained. Each substantially changed new release is accompanied by a new DOI and every release is supported by a change log.

Evidence:

****

F17 Ingest processing quick
reference http://www.data-archive.ac.uk/media/54764/ukda080-ds-processingquickreference.pdf
F15 Qualitative Processing
Procedures http://www.data-archive.ac.uk/media/54767/ukda093-ds-qualitativeprocessingprocedures.pdf
F16 Quantitative Processing
Procedures http://www.data-archive.ac.uk/media/54770/ukda081-ds-quantitativedataprocessingprocedures.pdf
W16 Curation process http://www.data-archive.ac.uk/curate/process

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

12. The data repository ensures the authenticity of the digital objects and the metadata.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

Ensuring that any alteration to the preserved version of any part of a data collection is accurately documented is integral to its authenticity.

Our Preservation Policy (link) includes the following definition of authenticity adapted from ISO15489 for Records Management: "A record's authenticity can be said to rely on three significant provable properties []: that the record is what it purports to be, that it was created by whomsoever it is purported to have been created by; and that it was created at the time when it is purported to have been created." The OAIS standard (link) states "Authenticity: The degree to which a person (or system) regards an object as what it is purported to be. Authenticity is judged on the basis of evidence."

The Preservation Policy definition of Migration requires that it "must maintain the authenticity, integrity, reliability and usability of any digital object"

While it is not feasible to guarantee the identities of all depositors no issue with depositor identification has been found. Pre-Ingest team members maintain close contact with many depositors and with the funding bodies. Funding identifiers are often collated alongside depositor contact details for data collections. The introduction of author identifier mechanisms support depositor identification and we recommend their use.

Our data offer form (**F03**) and deposit form (**F05**) both collect early provenance data critical to authenticity which is then maintained in the archive's data catalogue.

Thus the primary goal of the preservation policy is to ensure the long-term accessibility of electronic information while ensuring the highest level of authenticity of any formats disseminated. In effect this means that all the inherent qualities upon which their authenticity depends are preserved. An audit trail throughout the ingest process

ensures that all changes made to prepare dissemination and archival copies of data collections are recorded. Audit trail information relevant to end users is made available alongside the data collection. As well as an audit trail the ingest process includes an element of depositor accountability whereby depositors are informed of actions undertaken before the data collection is released.

From the point of internal custody transfer to Archival Storage stringent integrity checks (see Guideline 12) ensure that no unauthorised changes are made to the data or metadata.

Evidence:

****

F03 New Depositor Data Offer Form http://www.ukdataservice.ac.uk/media/455252/data_offer_form.docx
F05 Data Deposit Form http://ukdataservice.ac.uk/media/158537/data_deposit_form.docx

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

13. The technical infrastructure explicitly supports the tasks and functions described in internationally accepted archival standards like OAIS.

Minimum Required Statement of Compliance:

3. In progress: We are in the implementation phase.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

We benchmark our technical infrastructure against the OAIS reference model throughout the archival process and document where we vary from the model.

D07 OAIS Functional Entities with UK Data Archive amendments. http://www.data-archive.ac.uk/media/3727/D7-HLH-OAISFunctionalEntities-UKDAamends_01_00-NoKey.png

The diagram OAIS Functional Entities: Local Amendments indicates that:

- we include a 'pre-Ingest' process in addition to Ingest which takes responsibility from the first point of contact with a potential depositor to the internal custody transfer of a deposit to our Ingest team.

- we construct DIP during the Ingest process rather than creating them from AIP copies at the point of request from Access; this implies that we move a DIP for download to the Access function

In addition to the above under OAIS "complex Repackaging' and all 'Transformation' are performed under Administration supervision by the Archival Information Update function to ensure information preservation". At the Archive such file format transformations and other updates (whether to meet user needs for differing file formats or to move away from 'at risk' formats) are undertaken through 'on demand processing' by the Ingest team.

OAIS functions are mapped to our infrastructure as follows.

- Pre-Ingest maps to our Collections Development and Producer Relations team

- Ingest to our Ingest team

- Data Management to our Pre-Ingest, Ingest, Technical Service and Access teams

- Archival Storage to our Digital Preservation Systems and Security Team

- Preservation Planning to our Preservation Planning Manager role

- Administration is mapped into Preservation Planning and other functions

In addition to the Data Seal of Approval we were one of the first repositories to benchmark against the Open Archival Information System (Beedham, et al., Assessment of UKDA and TNA Compliance with OAIS and METS Standards (2005)) We undertook a test audit against ISO 16363 as part of the EU-funded APARSEN project (FP7 269977) and contributed to D33.1B Report on Audit and Certification. We are evaluating the possibility of a self-assessment against this standard and the German national standard DIN31644 (http://www.langzeitarchivierung.de/Subsites/nestor/EN/nestor-Siegel/siegel_node.html) in line with the European Framework for Trustworthy Digital Repositories (http://www.trusteddigitalrepository.eu). We are accredited to ISO27000 for Information Security which takes a risk management approach; we will evaluate how this could integrate with a DRAMBORA (http://www.dcc.ac.uk/resources/repository-audit-and-assessment/drambora) risk assessment. The UKDA has also led activities across CESSDA using the DSA to benchmark trust issues as preparation for their work plan.

We have participated in the development of the Data Documentation Initiative (DDI) standard commonly used in the social sciences and make DDI2.5 metadata available for harvesting alongside Dublin Core metadata.

Current infrastructure development plans at the archive include the redevelopment of business process and data/metadata management systems with:

- A 'schema-agnostic' metadata profile and relational database intended to support eventual XML export of a number of relevant metadata for harvesting and inclusion in AIP

- A registry of controlled vocabularies

Both of the above will sit alongside business process diagrams and procedural documentation as key artefacts for change management.

Evidence:

****

D07 OAIS Functional Entities with UK Data Archive
amendments http://www.data-archive.ac.uk/media/3727/D7-HLH-OAISFunctionalEntities-UKDAamends_01_00-NoKey.png

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

14. The data consumer complies with access regulations set by the data repository.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

From our perspective it can be challenging to separate this guideline on criteria in place to control access from guideline 15 on Use and Exchange of Information and guideline 16 on Usage Licence Compliance. In this self-assessment statement we will deal exclusively with the setting and enforcement of criteria for access, not to the subsequent use of data, though the licence evidence will cover wider issues.

Access criteria for data collections are set at the point of deposit in agreement with the data depositor. These may be based on:

The User

e.g. access may be restricted to higher or further education users based in the UK (UK HE/FE)

The intended use

e.g. restrictions on commercial use of data or a requirement to pay for commercial use of data

The Data

e.g. a user may need to accept additional conditions or receive additional permission or training to ensure they are an appropriate person with appropriate knowledge

e.g. the access method may be restricted to a secure online environment (SecureLab) or offline environment (Saferoom)

The applications of these distinctions into open, safeguarded and controlled data can be found in the self-assessment statement for guideline 16: Usage Licence Compliance.

Open data do not require users to register for an account (login/password) but may be subject to an Open Government Licence (OGL) or a Creative Commons Licence (CC).

Safeguarded and Controlled data require users to be registered. Users who register have to accept our End User Licence (EUL) which is agreed to during the registration process.

User information relating to UK HE/FE status may be detected through metadata available through the UK Federation Shibboleth single-sign on system (http://www.ukfederation.org.uk/)

Additional user information relevant to access may be requested at the the point of registration

When a user requests access to a non-Open data collection their intended use is collected if relevant. This guides whether access will be permitted.

The access criteria assigned to the data will then direct the user making an access request through an appropriate 'order' process which may include the acceptance of additional conditions or the provision of additional information.

In some cases access can be granted immediately in an automated way based on information provided, in others the request is passed to our Access team. The Access team will arrange additional permission from the depositor and arrange any training required before access. Access to data is then permitted via download, or arrangements are made to use appropriate secure access routes.

Until access permission is granted the data are protected under information security conditions compliant with and registered to ISO27000. Violating the access conditions would entail a breach of our technical security (hacking) or physical security (entering a secure office or server space) either of which could be subject to criminal prosecution.

Evidence:

****

W19 Terms and Conditions of Access http://ukdataservice.ac.uk/conditions.aspx
W20 Open Data http://ukdataservice.ac.uk/get-data/data-access-policy/open-data.aspx
W21 Safeguarded Data http://ukdataservice.ac.uk/get-data/data-access-policy/safeguarded-data.aspx
W22 Controlled Data http://ukdataservice.ac.uk/get-data/data-access-policy/controlled-data.aspx
F19 End User Licence http://ukdataservice.ac.uk/media/455131/cd137-enduserlicence.pdf

F11 Licence Compliance Policy http://ukdataservice.ac.uk/media/311391/CD142-LicenceCompliancePolicy.pdf

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

15. The data consumer conforms to and agrees with any codes of conduct that are generally accepted in the relevant sector for the exchange and proper use of knowledge and information.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

From our perspective it can be challenging to separate this guideline on the use of data by users from guideline 16 on Usage Licence Compliance. In this self-assessment statement we will deal exclusively with use and exchange issues not covered by usage licences.

The setting, communicating and enforcing of codes of conduct is generally a matter for professional bodies, host institutions and funding organisations. In addition to these there are legal requirements for the use and exchange of data. Complying with such codes and legislation remains a matter for the individual data user though we work to communicate relevant information about such guidance and on good practice in working with research data of all types including that pertaining to human subjects. Staff identifying use or exchange of information which violate a code of conduct or legal edict would be under the same obligation as any other member of the public to report this to the appropriate authority.

Our terms of use to which subjects agree, including additional restrictions such as commercial or teaching use are all contained within user licences and will be addressed under Guideline 16.

We do not undertake ethical evaluation of work which leads to the creation of data, our funder, the Economic and Social Research Council (ESRC) provides detailed guidance to ensure that research they fund is designed and conducted in accordance with recognised best practice and ethical standards and subject to proper professional and institutional oversight in terms of research governance (http://www.esrc.ac.uk/about-esrc/information/framework-for-research-ethics/).

Our role in the protection of human subjects is in ensuring that data are appropriately anonymised and that access is granted under conditions which reduce the risk of disclosure.
Extensive guidance and resources are made available to both data producers and data users covering the ethical use and exchange of data including legal issues, consent and anonymisation.

Evidence:

****

ESRC Framework for Research Ethics (R05, R02)

Ethical Guidance (W06)

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments:

16. The data consumer respects the applicable licences of the data repository regarding the use of the data.

Minimum Required Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Applicant Entry

Statement of Compliance:

4. Implemented: This guideline has been fully implemented for the needs of our repository.

Self-assessment statement:

From our perspective it can be challenging to separate this guideline on the use of data by users from guideline 14 on Access Criteria and guideline 15 on Use and Exchange of Information . In this self-assessment statement we will deal exclusively with the rights and obligations of data use required by licences, not the access process or on more general ethical data use.

An overview of terms and conditions for access can be found at **W19** with full details at **W23**. Licences are based on the (contract) laws of England and
Wales and national (United Kingdom) legislation where appropriate. Other licences/agreements are in place for disclosive data to meet the requirements of the Statistics and Registration Service Act (2007)

Open data do not require users to be registered with us but may be subject to an Open Government Licence (OGL) or a Creative Commons Licence (CC).

An End User Licence (EUL) is agreed to during the registration process. Safeguarded data require users to be registered, and access may be subject to permission from depositors. Controlled data may require that users accept conditions of use in addition to those contained in the EUL.

Once users have been permitted access to data we have limited capability for monitoring its eventual use and on enforcing penalties if conditions of use are not complied with. For data restricted to access via safe room or SecureLab use can be monitored and any research outputs derived from the data are reviewed by our staff before release to ensure compliance with terms of use.

One basic obligation of use is to give appropriate credit to the data used in future work via citation (format supplied with all data). We cannot realistically enforce this but make it as easy as possible and actively promote the benefits of citation to the whole data using community (**W15**).

Breaches of licence conditions relating to the use of data can result in a range of outcomes if they come to our attention ranging from informing the original data producer/depositor contact (e.g. if attribution requirements for OGL or CC licences are not adhered to), to termination of access to data (or requirement that downloaded data be destroyed), to restrictions (permanent or time limited) on future access to data which we hold.

Usage conditions which could be breached include use of data for commercial purposes without permission. Some types of violation of terms of use, e.g. attempts to identify individuals or the sharing of data beyond approved researchers, could be subject to legal penalties.

Evidence:

****

W19 Terms and Conditions of Access http://ukdataservice.ac.uk/conditions.aspx
W23 Full Conditions http://ukdataservice.ac.uk/get-data/how-to-access/conditions.aspx
W15 Citing Data http://ukdataservice.ac.uk/use-data/citing-data.aspx

W20 Open Data http://ukdataservice.ac.uk/get-data/data-access-policy/open-data.aspx
W21 Safeguarded Data http://ukdataservice.ac.uk/get-data/data-access-policy/safeguarded-data.aspx
W22 Controlled Data http://ukdataservice.ac.uk/get-data/data-access-policy/controlled-data.aspx
F19 End User Licence http://ukdataservice.ac.uk/media/455131/cd137-enduserlicence.pdf

****

Reviewer Entry

Accept or send back to applicant for modification:

Accept

Comments: