Research data handling and security guide for users



12 November 2026

Public

Copyright © 2026 University of Essex. Created by UK Data Archive, UK Data Service.

Version: 19.00

CC BY-NC-SA

Table of contents

1. Scope 4
2. Data licence and access framework 4
2.1 End User Licence Agreement 5
2.2 Safeguarded data 6
2.2.1 Special conditions 6
2.3 Controlled data 6
3. Accessing data 7
3.1 Research projects and teams 7
3.2 Teaching purposes 7
3.3 Reuse of data 7
3.4 Security 7
4. Data storage and security 8
4.1 Safeguarded data 8
4.1.1 Safeguarded Special Licence data 8
4.2 Controlled data 9
4.2.1 Access via SecureLab 10
4.2.2 Access via the UK Data Service's Safe Room 11
4.2.3 Access via the SafePod Network 11
4.2.4 Access via an IDAN secure data access point 12
4.3 Passwords and passphrases 12
4.4 Audit of confidentiality and security procedures 12
4.5 Use of online data tools 12
4.5.1 Context and definitions 12
4.5.2 Key risks associated with online data tools 13
4.5.3 Applying for permission (case-by-case assessment) 13
4.5.4 Locally deployed AI tools 14
5. Statistical disclosure 14
5.1 Data matching 14
5.1.1 Safeguarded data 14
5.1.2 Controlled data 15
5.2 Outputs 15
5.2.1 Safeguarded data 15
5.2.2 Controlled data 16
6. Citing data and reporting publications 17

7. When research is complete 17
7.1 Guidelines on data destruction 17
8. Organisational responsibilities 18
8.1 Safeguarded Special Licence data and Controlled data 18
9. Non-compliance procedures 19
10. Help and feedback 20

1. Scope

This guide is for users of research data accessed via the UK Data Service (the Service) through its online services. In particular, all users who obtain data available subject to the Service End User Licence Agreement, and any other Service conditions or Agreements, are required to read, understand and follow the guidance in this document.

In this document, we use the term *Safeguarded* data to describe effectively anonymised data[1]. *Controlled* data is used to describe data defined as personal data under the Data Protection Act (2018) and the UK General Data Protection Regulation (UK GDPR) or personal information as defined in section 39(2) of the Statistics and Registration Service Act 2007, subject to the Secure Access User Agreement and are made available through the Five Safes framework[2]. Use of Safeguarded and Controlled data is subject to the Service End User Licence (EUL) Agreement.

2. Data licence and access framework

The Service does not own the data collections held in its repositories. All data collections available via the Service are negotiated with data depositors to be curated, preserved, and shared on their behalf. Data depositors, or their nominees, agree the terms of access and use for the collections they deposit with the Service.

A legal and ethical framework designed to protect the rights of data subjects and data creators binds all users accessing these data. Users have responsibilities to observe the ethical and legal obligations pertaining to the data as defined by the licences under which these are made available.

The conditions under which data may be accessed are specified in the deposit licence and are set out clearly for users in the catalogue record's 'Access data' tab.

The Service operates a three-tier licence and access framework as follows:

Open data

- These data are either not related to individuals (e.g. aggregate data), have been modified in such a manner that individual identification is impossible, or consent to public disclosure is in place. These data are made available to any user without the requirement for registration for download/access.
- Use of these data are subject to Open Licences such as the Open Government Licence or Creative Commons variations.

[1] ico.org.uk/media2/migrated/4018606/chapter-2-anonymisation-draft.pdf
[2] ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/

Safeguarded data

- These data may be related to individuals, but the risk of identification is considered sufficiently remote. These are made available to registered, authenticated users, and where appropriate, special conditions are agreed to ahead of access. These data are effectively anonymised.
- Use of the data is subject to the UK Data Service End User Licence Agreement; additional agreements might apply.

Controlled data

- These data are either personal information, personal data, or data that are particularly sensitive, commercially or otherwise. These data are available only on request to registered, authenticated and accredited users.
- Use of data is subject to the UK Data Service End User Licence Agreement and the UK Data Service Secure Access Agreement and access is facilitated via the Five Safes framework; additional agreements might apply.

2.1 End User Licence Agreement

Use of Safeguarded and Controlled data is governed by a legally binding End User Licence Agreement. Everyone who requires access to Safeguarded or Controlled data has to register with the UK Data Service. Users who are part of the UK Higher/Further Education (UK HE/FE) sector or those based at an institution that is part of the UK Access Management Federation (UKAMF) will be able to utilise their institutional credentials to complete the registration and enter into the End User Licence Agreement. Others can apply for UKD credentials via the Service.

Under the terms of the End User Licence Agreement, users agree:

- To use the data only for the specified purposes as declared in their project and not to share it with unauthorised users.
- To abide by any further conditions of use as imposed by the data owner.
- To preserve the confidentiality of, and not attempt to identify, individuals, households or organisations in the data as applicable.
- To ensure that the means of access to the data (such as passphrases) are kept secure and not disclosed to anyone else.
- To refrain from uploading or processing the data collections using online data tools without prior written permission from the Service.
- To comply with statistical disclosure control standards described in this guide for any outputs they might publish.

- To securely delete all the data at the end of their project using methods described in this guide.
- To use the citation and acknowledgement information provided by the Service, in all publications.
- To supply to the Service, the bibliographic details of any published work based on the data collections.

2.2 Safeguarded data

2.2.1 Special conditions

For some data collections, data owners may specify special conditions of use in addition to those agreed in the End User Licence Agreement. These include click-through additional conditions, depositor permission applications and Special Licence User Agreements. At all times, users must ensure they abide by all conditions of access they have agreed to.

2.2.1.1 Additional conditions

Users are prompted within their access requests to agree and sign to any additional conditions and must follow any steps required for accessing data.

2.2.1.2 Safeguarded Special Licence data

Safeguarded Special Licence data (Special Licence data) are effectively anonymised but require additional safeguards. Access to these data may be restricted to certain users depending on the data owners' requirements, for example, those working within the UK or in countries deemed by the UK to have an adequate level of data protection or researchers based in Higher Education/Further Education institutions.

Users wishing to access these data must complete an application which needs to be approved by the data owner or their nominee. Users also must agree, sign and submit a Special Licence User Agreement.

Data explicitly defined as **personal data** under the UK GDPR are not made available as Safeguarded data.

2.3 Controlled data

Controlled data (also referred to as Secure Access) are only available through the Trusted Research Environment provided by the Service, the UK Data Service SecureLab, and/or the UK Data Service Safe Room, and via the ESRC SafePod Network.

Any registered user requiring access to Controlled data will have to (i) be accredited as an ESRC and/or Digital Economy Act Accredited Researcher, (ii) complete the Safe Researcher Training (SRT) and pass the training test, and (iii) agree to the Secure Access User Agreement. A project application must be submitted and approved by the data owner or their nominee.

3. Accessing data

All users should ensure they understand the terms under which the data are made available to them for reuse. All conditions must be met at all times and users are encouraged to contact the Service if they have questions.

For example, under Open Licences there might be restrictions on commercial use and derivative work; for Safeguarded data, additional conditions of use might be imposed, which have to be agreed to before access is granted. It is the users' responsibility to ensure all terms and conditions of use are respected.

3.1 Research projects and teams

Users are required to register research projects via their online UK Data Service account. A research project can comprise of a single user or a project team. The information provided by the project lead must be comprehensive, and if there are any scope changes in the project, users need to ensure they update their project descriptions.

The period of access is typically set by the data owner but tends to be between two and five years. Users should contact the UK Data Service Helpdesk if they wish to extend a project.

Where a user joins a research team that has already been granted access to Safeguarded Special Licence data or Controlled data, they must follow all access steps as their colleagues on the project, including completing necessary application forms, additional user agreements or training and their data use being formally approved by the Service.

The Service will provide advice on the process to be followed, which is largely self-prompted within the user account system.

3.2 Teaching purposes

When using data for teaching purposes, the tutor must sign and return the Teaching Agreement and/or ensure that all students are registered with the UK Data Service.

Safeguarded Special Licence data and Controlled data cannot be used for teaching.

3.3 Reuse of data

Reapplying for access will be required for reuse of anything but Open data already supplied, if used for a different purpose. All data usages are assigned to a dedicated project in a user’s account. Any new project will need to be registered and data added. Where a data owner’s permission is required, this will need to be obtained again for a new project.

Using data for a different project is a non-compliance with the End User Licence Agreement and is subject to penalties.

3.4 Security

Passwords and passphrases that provide access to UK Data Service data or computing

environments must never be disclosed to anyone else. Data must never be stored on a computer that might enable unauthorised access.

4. Data storage and security

4.1 Safeguarded data

Safeguarded data provided by the Service must be stored under conditions that meet the undertakings given in the End User Licence Agreement (see section 8 for organisational responsibilities) and those listed below. Additionally, users should be aware of any **specific information security guidelines** provided by their organisation.

Authentication

- Regardless of whether data are stored on endpoint devices (e.g. PC, laptop, thin client, virtual machine) or on cloud platforms (Box, Google, AWS etc.), the use of shared credentials is strictly prohibited. Each user must have their own individual login credentials, including a unique username and password or passphrase, to access the data storage location (see section **Error! Reference source not found.** for further details on passwords and passphrases).

Storage

- For studies restricted to specific geographical locations, data must only be stored in the countries explicitly specified for that study. This condition must be strictly adhered to. When using a cloud platform for storage, **the platform must store the data within these specified countries**. Where studies are restricted to specific countries, these will always be defined in the catalogue metadata, in the "Access study data" information on the left-hand side of the catalogue record for each study. If in doubt, users should contact the Service.

Encryption, passwords and passphrases

- Means of access to the data (such as passwords or passphrases), including the UK Data Service account credentials, must be kept secure and must not be shared with anyone.
- Data on portable media (e.g. a backup on a USB memory stick) must be encrypted using a strong secure password or passphrase.

Data deletion

- Data **must be deleted** upon project completion as set out in section 7. Failure to delete, continuing to use data and/or using data for an unauthorised project constitutes a non-compliance as per the End User Licence Agreement and is subject to penalties.

4.1.1 Safeguarded Special Licence data

In addition to the responsibilities described above, Safeguarded Special Licence data have some additional requirements around safe data storage and handling.

Where a Data Management Plan has been created for a research project, it is useful to refer to any processes agreed with your organisation, and to include these in the project application.

Storage

- Users must only store the data on devices that belong to the declared institution/organisation. Personal devices are not permitted for storing the data. The device must have a current supported operating system, which has all security patches installed and automatically applied. The device must have anti-malware installed with updates automatically applied.
- Alternatively, data may be stored on a non-local platform, such as a network server or a cloud service, provided that the platform is managed by the institution/organisation and complies with the security standards described in this document.

Access location

- Users must declare their institution/organisation address as the designated location for accessing the data. Data access is restricted to this declared location. **Accessing the data from any location other than the declared institution/organisation address is strictly prohibited unless explicit permission has been requested and granted** by the Service.
- Data are only be accessed at locations where they have been approved by the data depositor or their nominee.

Encryption, passphrases and screen locks

- The data must be encrypted at all times when not in use, using strong passphrases.
- The device used must be protected by a screen lock that activates after no more than fifteen minutes of inactivity. Unlocking the screen must require a secure password or passphrase.

Data deletion

- Besides the standard deletion requirements, the data destruction form must be completed fully and returned to the Service. Failure to return the form constitutes non-compliance with the terms and conditions of the Special Licence User Agreement.

4.2 Controlled data

The UK Data Service provides four methods of access to Controlled data:

- Remotely from the user's organisation or via an institutionally-approved secure

connection method.

- From the Service's Safe Room, physically located at the UK Data Archive in Colchester.
- Via the ESRC SafePod Network (SPN) 'SafePods', installed in some institutions around the UK.
- Via an International Data Access Network (IDAN) secure data access point.

4.2.1 Access via SecureLab

Data accessed remotely via the SecureLab must only be accessed from a designated office at an organisational/institutional site; if working from home permission has been applied for and granted, access is permitted via an institutionally-approved secure connection method.

Data accessed from a designated office at an organisational/institutional site can only be accessed from an endpoint device that:

- Is managed by the institution or managed by another party on behalf of the institution from which the SecureLab will be accessed. Personal devices must not be used.
- Has a current operating system that is receiving security updates which are automatically applied within 14 days of release.
- Has anti-malware software installed and updated automatically.
- Has a direct connection to the internet via a wired Ethernet connection or a wireless connection with WPA2/3 encryption managed by the host organisation.
- Has no other network interfaces connected except for the one being used to access the SecureLab.
- Is not running any services which allow third parties external to the institution to connect to the workstation, e.g. remote control software, a web server or an email server.
- Is not running screen capture tools.

Data accessed from home, where explicit permission has been granted, can only be accessed from an endpoint device that:

- That meets the same criteria as the endpoint device that is located at the organisational/institutional site as above.
- Uses an organisationally/institutionally approved secure connection method of remotely accessing the organisational/institutional located endpoint.

Users accessing data via their SecureLab, accounts do not have the technical functionality to

transfer, download, copy and paste any data, or print to a local computer. Users must not copy screenshots to a local computer.

Good security measures must be observed by the user, for example:

- Locking screens when leaving the computer unattended.
- Not allowing screens to be visible to people other than SecureLab users working on the same SecureLab project.
- Credentials must not be saved or cached in the web browser.

Outputs from analysis of the data within the SecureLab are only released to the user subject to statistical disclosure control checks undertaken by Service staff. Users are **strictly forbidden from copying anything from the screen**. Controlled data and outputs must not be seen on the user's computer screen by unauthorised individuals. However, the use of whiteboards in approved secure environments, such as Safe Rooms and SafePod Network environments, is permitted, provided such use is in line with the specific operational procedures of the respective environment.

Users who have been approved to work together on the same project may only share unchecked outputs from that project with each other in the relevant shared project area within the SecureLab. Temporary or duplicate files should be deleted by the user(s) from the SecureLab. The SecureLab user guide provides detailed advice on managing work in the SecureLab.

All user activity within SecureLab is recorded to provide the Service with information about any suspicious activity and for auditing purposes.

4.2.2 Access via the UK Data Service's Safe Room

The conditions under which data are accessed via the UK Data Service's Safe Room are similar to those for accessing the SecureLab remotely. However, access via the Safe Room differs from remote access in that:

- Access is only available from within the room.
- Thin-client terminals are used to access the Servers where the data are held.
- Users must abide by the procedures, listed in the *Safe Room procedures* document (CD226-SafeRoomProcedures).

4.2.3 Access via the SafePod Network

The conditions under which data are accessed via the SafePod Network are similar to that of the Safe Room.

- Sessions must be booked via the SafePod Network.

- Users must abide by the SafePod Network procedures.

4.2.4 Access via an IDAN secure data access point

The conditions under which data are accessed via an IDAN secure data access point are similar to that of the Safe Room. Users can find information regarding data availability at our International Data Access Network (IDAN) web page. Users are advised to consult the guide UKDS SecureLab: access to non-ONS data for researchers outside of the UK via Safe Room Remote Desktop Access.

- The IDAN access points must be booked via the partner organisation.
- Users must abide by the Licence Compliance Policy of the partner organisation access point.

4.3 Passwords and passphrases

Passphrases differ from passwords in format and in length. Passphrases are usually much longer, up to 100 characters or more and may contain spaces. The greater length and format of passphrases makes them more secure. Wherever possible we expect passphrases to be used.

A password should be at least 16 characters long. It must not contain usernames or personal information, such as date of birth, address, phone number or family or pet names.

4.4 Audit of confidentiality and security procedures

The Service and the data owners reserve the right to conduct an onsite audit and the right of entry to the premises where the data are stored and/or accessed (see section 8). The Service and data owners may request a copy of the licence holder's security audit report if applicable and/or the licence holder's confidentiality and security procedures).

4.5 Use of online data tools

4.5.1 Context and definitions

We define online data tools as any software, application, web service, or cloud-based platform that operates via the internet to process, analyse, clean, manipulate, or generate data and supporting documentation.

These platforms increasingly incorporate Artificial Intelligence (AI) and Generative AI (Gen AI) technologies designed to perform tasks such as natural language processing, automated coding, text summarisation, and content generation. We fully recognise the potential of these platforms to boost research efficiency, enhance productivity, and support innovative research methods.

However, safeguarding data security and intellectual property rights remains paramount. Under Clause 5 of the End User Licence Agreement uploading or processing data collections using online data tools **without explicit prior written permission from the Data Service**

Provider is strictly prohibited.

4.5.2 Key risks associated with online data tools

The broad restriction is designed to protect researchers and data owners against two main risks:

- Loss of data and operational control: web-based and browser-integrated tools frequently process data on external servers. This makes it impossible to guarantee compliance with data-hosting standards, or strict confidentiality obligations. This also makes it impossible to delete the materials in line with the End User Licence Agreement conditions and the guidance described in section 7 of this guide.
- Intellectual property and copyright loss: some public or standard web-based AI tools operate under terms of service that grant the vendor rights to store, re-use, or train future foundation models on user inputs. Uploading data or even documentation and metadata such as questionnaires into unapproved tools can permanently compromise copyright.

4.5.3 Applying for permission (case-by-case assessment)

We do not enforce a blanket ban on modern research tools; rather, we manage risk through a structured review process. Permission is frequently granted where the risk profile is low and appropriate safeguards are demonstrated.

We recognise that a growing number of organisations are now deploying enterprise-grade, versions of online data tools including AI and GenAI assistants. While these "walled-garden" environments offer robust data protection and zero data-retention guarantees, **written confirmation from the Service is still required before data are uploaded.** This step is strictly to verify that the specific institutional deployment is configured in full compliance with the End User Licence Agreement requirements.

To help us assess your request without delay, please contact the UK Data Service using the contact form and supply:

- The exact platform, version, and account type: Specify whether you are using a free consumer account, a paid personal subscription (e.g. ChatGPT Plus, Claude Pro), or an institutionally managed enterprise account (e.g. Microsoft 365 Copilot Enterprise, Azure OpenAI).
- The exact materials you plan to upload: Clearly distinguish between a) raw/individual-level data (including synthetic data derived from the collection), b) documentation/metadata (e.g. questionnaires, codebooks), or c) disclosure-checked aggregate data and statistical outputs.
- Evidence of data-handling controls: Confirmation from the provider's terms of service or your institution's agreement that:

1. Prompts, uploads, and outputs are not used for model training.
2. Content is not persistently stored by the vendor.
3. The vendor makes no copyright or intellectual property (IP) claim over your inputs or outputs.

- Your intended outcome and how the tool will be used.

There may be instances where we may need to consult directly with the data owners to determine whether the proposed use is permitted. Users should allow appropriate lead time for these reviews.

Please note: Uploading raw data, individual-level derived data, including synthetic data versions, into free or paid personal consumer AI accounts is strictly prohibited, even if model training is toggled off in your user settings. Raw/individual-level data can only be considered for use within institutionally managed enterprise environments.

4.5.4 Locally deployed AI tools

Tools that run entirely locally on your device or local institutional server, where you retain complete control over data storage, processing, and deletion, and where no data is transmitted externally over the internet, are not classified as online data tools and therefore can be used without permission as long as all the End User Licence Agreement clauses are respected.

Note that desktop applications which act as a front-end interface for cloud-based AI (such as the standard Microsoft Copilot desktop app) still transmit data to external servers and remain subject to permission.

If you are ever uncertain about whether a tool transmits data externally, or if you need advice, please contact the Service for guidance prior to deployment.

5. Statistical disclosure

5.1 Data matching

Data matching can increase the risk of the disclosure of personal information and is therefore only permitted under certain circumstances. This must be declared in applications, where appropriate.

5.1.1 Safeguarded data

Where Safeguarded data are matched with external data sources this must not be for the purposes of re-identification. The terms and conditions of the End User Licence Agreement explicitly forbid the use of any methods that will lead to the re-identification of participants.

5.1.1.1 Safeguarded Special Licence data

Any plans to match or attempt to match individual or household records to any other data

source at the level of the individual or household must be declared in the project application. This level of analysis can only be undertaken with the explicit permission of the relevant data owners.

5.1.2 Controlled data

Whilst the SecureLab provides an area in which secure data could be linked (e.g. with another dataset in the controlled collection or with the user's own data) this is strictly subject to the explicit permission of the data owner. Users will only be able to access those datasets approved for a particular research project. It will not be possible to subsequently add new data without a revised application and subsequent approval.

ONS business data may be linked using the anonymised reference numbers (known as IDBR references). A user may be able to produce a larger 'combined' dataset, with many variables providing characteristics that will directly identify an organisation. While this is an acceptable risk within the confines of the SecureLab, users must be aware that output requests containing information that will identify an organisation, will be rejected (see section 5.2).

5.2 Outputs

All outputs resulting from analysis of Safeguarded and Controlled data must be subjected to statistical disclosure control (SDC) checks and treatment. Further attention must be given to Safeguarded Special Licence data and Controlled data. Users must refer to detailed procedures in the following best practice guidance documents:

- The Government Statistical Service's 'Disclosure control for tables produced from surveys'.
- The Safe Data Professional Group's 'Handbook on Statistical Disclosure Control for Outputs'.

There are some differences between SDC management for Safeguarded and Controlled data. The latter may be created from personal data, much more granular and sensitive, hence outputs must be checked by the Service before being released.

5.2.1 Safeguarded data

Some simple rules of thumb apply; these must be applied to any Safeguarded data:

1. **Tables that contain very small numbers in some cells may be disclosive.**

- Tables must never report numbers or percentages for cells based on only one or two cases; this is known as a minimum threshold of 3 and avoids primary disclosure. Cells based on one or two cases must be combined with other cells or, where this is not appropriate, reported as zero per cent.
- To avoid secondary disclosure, especially when multiple outputs are presented from the same data source, users are advised to use a higher threshold i.e. 10.

- Users should always adhere to any additional conditions imposed on outputs e.g. some studies require a minimum threshold of 30.

2. **Tables and other outputs must not be published in a form where the level of geography would threaten the confidentiality of the data.**

- Whenever possible the geography in any published outputs should not be lower than Region/UK Government Office Region (GOR). Where there is a fully justified requirement to publish outputs at a lower level of geography then the user must assess and ensure there is no risk of disclosure.
- Where there is any doubt, the user must contact the UK Data Service via the Helpdesk to obtain confirmation of the acceptability of publication of the output.

3. **Care must be taken to ensure that individuals, households, or organisations cannot be identified in models or other statistical analysis**.

- Results based on very small numbers must be avoided; summary and test statistics such as R-square, t, F, chi-square must only be presented where there are at least N degrees of freedom in the model, where N is the set threshold.
- Any output that refers to unit records, e.g. a maximum or minimum value, must be avoided.
- Models must not report actual values for residuals (as each residual constitutes a single observation).

4. **Graphical outputs must be based on non-disclosive data.**

- Particular care must be taken not to report extreme outliers.

5.2.2 Controlled data

The SDC requirements for Controlled data differ from those mentioned above for Safeguarded Special Licence data.

Access to Controlled data is only available through the SecureLab. Users must conduct all their analysis, and produce their research outputs (such as papers, presentations etc.) within their dedicated project area. Controlled data will not be released to be used in any other environment under any circumstance.

Users must maintain familiarity with SDC. The two guidelines above offer detail on checking, but users will be given mandatory Safe Researcher Training that covers most of the key concerns around routine analytic outputs. A detailed SecureLab user guide is also available that SecureLab users should read and digest.

Outputs will be returned to users following a full SDC examination by two trained members of Service staff. It is the policy of the Service to only release ‘final results’ which are those

considered ready for publication or a formal presentation. This avoids multiple attempts at clearing outputs, and is achievable because users working on the same project in the SecureLab can share their intermediate findings through shared project folders.

Where users are unsure about SDC when they produce outputs, we recommend that they speak to a Service support officer as soon as possible, and certainly before any outputs are submitted for checking. This will avoid disappointment if a user writes an entire paper within the secure environment, only to find that it is not released to them due to SDC problems.

6. Citing data and reporting publications

As outlined in the End User Licence Agreement, all users of data are required to cite the data, including using the Digital Object Identifier (DOI) of the dataset(s) in any publications or presentations arising from their research using collections from the Service. The Service should be informed of any publications and be provided with the full citation and DOI of the work. These publications can then to be added to the data catalogue record to provide useful information for new users.

Owners of data may reserve the right to ask to see or vet drafts of publications based on those data prior to publication. This will be noted in the Access conditions and users are notified during the application process.

Users of the SecureLab are not permitted to publish outputs unless they have been checked and released to them as outlined in section 5.2.2. If data owners wish to vet publications, users will be notified in advance.

7. When research is complete

It is recommended that users always retain a well-documented copy of any data preparation or analytic code used in their work.

For Safeguarded data when a project has been completed, users must delete all copies of the data, including derived datasets, backups, paper copies, portable copies (including CDs), and all electronic copies from every device, and any Server, used. Additionally for Safeguarded Special Licence data the Service must be notified of the destruction via the completion of a Data Destruction form.

Users of Controlled data must ensure that their code files are stored in the ‘Syntax Folder’, which will be retained at the end of the project’s life. All other files will be deleted at the end of the project. Code files can be removed from the SecureLab subject to clearance checks by Service staff.

7.1 Guidelines on data destruction

The following guidelines for destroying data must be adhered to:

- Data must be deleted from the system on which it has been stored using a secure erasure programme, such as Eraser or similar — which repeatedly overwrites files a

number of times, until such time as the original data could not be retrieved forensically.

- The recycle/trash bin must be emptied, preferably to be immediately followed by running a secure erasure program; portable media holding any data must be destroyed and disposed of in a secure manner.
- Backup tapes must either be completely overwritten and degaussed (demagnetised) before being reused or disposed of.
- Paper copies must be destroyed by shredding, preferably using a cross-cut shredder.
- Before the PC, laptop or other device used for data storage leaves the possession of the organisation or individual (for destruction or second-hand sale, etc.), the hard disk must be completely erased using a secure erasure programme.
- Destruction of Safeguarded Special Licence data must be confirmed to the Service by the user. A Data Destruction form will be sent to the user one month before the project expires.

8. Organisational responsibilities

UK Institutes of Higher or Further Education are bound by JANET policies, including the JANET Security Policy that places responsibilities on every person and organisation involved in the use or operation of JANET to protect the network against security breaches.

Most organisations have their own Information Security policies, which should be consulted before requesting access to data subject to the Safeguarded Special Licence data. If there is any doubt that your organisation has lower standards than those suggested here, you should check with your IT Services department.

There is a requirement that all central government departments must meet internationally recognised information and security management standards (e.g. ISO/IEC 17799 and/or ISO 27001) for their systems. Local authorities are also obliged to comply with the ISO 27001 security standard as part of their Implementing Electronic Government (IEG) requirements.

8.1 Safeguarded Special Licence data and Controlled data

For a user accessing Safeguarded Special Licence data, it is the user's responsibility to ensure that they can store and access the data in a suitably secure physical and electronic environment.

Users of the SecureLab must provide a Secure Access User Agreement which needs to be signed by an authorised signatory of the user's organisation (usually the Registrar or delegate). In accordance with the agreement, the Service maintains the authority to oversee, document, and evaluate the use of personal information and data. The Service reserves the right to access the premises where the data are being used to ensure adherence to the

technical requirements needed to access the SecureLab.

Access to Safeguarded Special Licence data and Controlled data may require the user to provide the contact details of a senior member of staff at their organisation who can vouch for their suitability for access to the data. The Service and data owners reserve the right to contact the senior member of staff to ask for a reference.

9. Non-compliance procedures

The user is required to promptly report any non-compliance with any of the terms of the End User Licence Agreement, Special Licence User Agreement or Secure Access User Agreement (this includes any non-compliance by someone else that the user becomes aware of). Failure to disclose an act of non-compliance is a non-compliance with the licence(s).

All users must consult the UK Data Service Licence Compliance Policy.

Non-compliance with the terms of the End User Licence Agreement, including any additional conditions, may result in the following actions:

- Immediate termination of access to all services provided by the Service and the UK Data Archive either permanently or temporarily.
- Legal action being taken against the individual who has not complied with the terms of the End User Licence Agreement.
- Withdrawal of access by the user's organisation to all Service and UK Data Archive services either permanently or temporarily.

Additionally, any non-compliance with the terms of access for Controlled data:

- Will result in the immediate termination of the user's access to the data and termination of the licence; depending upon the seriousness of the non-compliance, the termination of access may be permanent.
- May result in sanctions being sought against the user by the data owner.
- Will, for ONS Controlled data under the Statistics and Registration Services Act 2007 and the Digital Economy Act 2017, incur penalties as specified within the Acts, which may include a fine and/or imprisonment.
- Penalties could also include individual or organisational sanctions including withdrawal of UKRI funding and organisational suspension from all UKRI data services, a fine and/or imprisonment.

Users will be provided with detailed guidance on non-compliance and penalties when undertaking the SecureLab training.

10. Help and feedback

This guide is updated regularly. For further advice, or to provide suggestions or comments, please contact the UK Data Service Helpdesk via our contact us web page.

www.ukdataservice.ac.uk

help@ukdataservice.ac.uk

We are supported by the Universities of Essex, Manchester, Edinburgh, University College London and Jisc. We are funded by UKRI through the Economic and Social Research Council.