SWANSEA UNIVERSITY MEDICAL SCHOOL

DATA RETENTION POLICY

Version	0.2 (DRAFT)
Issued By	ROB GARLICK
Classification	OPEN
Review Date	27/02/2023
Status	PENDING APPROVAL
Reference	SAIL-POL-0036
Note	UNCONTROLLED WHEN PRINTED

CONTENTS.

PURPOSE. 3
SCOPE. 3
1. SAIL PROGRAMME DATA RETENTION POLICY 3
1.1 SAIL Data Retention purpose 3
1.2 Retention Schedule 3
1.3 Data deletion process 6
1.4 Audit of data retention 6
2. SAIL DATA RETENTION - ROLES AND RESPONSIBILITIES. 6
3. SAIL DATA RETENTION - COMPLIANCE. 7
A. DOCUMENT MANAGEMENT 7
A.1 AUTHORISATION. 7
A.2 DISTRIBUTION. 7
A.3 REFERENCES. 7
A.4 DOCUMENT HISTORY. 7

PURPOSE.

This document has been created to clarify the retention periods around personal identifiable data held by SAIL and the justification for these conditions. Whilst SAIL is part of Swansea University (and therefore subject to the retention schedule set by the university), there are certain types of identifiable data unique to SAIL operations which must be obtained to support SAIL services and to provide an audit trail.

SCOPE.

This document does not cover document retention arrangements relating to SAIL where a centralised university process resulted in the document being obtained or generated. In these cases, the university already has retention arrangements in place for this documentation and has designated departments which are responsible for managing this information. Examples of such documents that are out of scope are CVs (relating to staff recruitment), staff disciplinary records, staff contract information etc.

This document does not cover non-identifiable data, as retention schedules are not a statutory requirement for this kind of data. SAIL research data is included within the list below, but this is for illustrative purposes.

The scope of this document covers any personal data which is obtained or generated to serve a specific SAIL operational purpose (such as project governance).

1. SAIL PROGRAMME DATA RETENTION POLICY.

The following sections detail the SAIL Programme retention schedule for personal identifiable data. Where possible, retention periods have been aligned to those set out in the JISC guidance for university document retention (which Swansea University's own retention policy adheres to).

The content of this policy will be reviewed annually to ensure that it remains up to date and covers the full range of data obtained or generated for SAIL operational purposes. This review will ensure that the policy accounts for any updates to the SAIL service which results in new data being utilised.

1.1 SAIL Data Retention purpose

The SAIL Databank must only retain personal data within the scope of this policy for a specific purpose. This policy will clarify these purposes and will provide information to those to whom the data relates as to the reasons behind any retention.

The SAIL team must notify the Information Security team of any instance where this retention policy has not been adhered to so that this can be rectified. This notification should be raised via the helpdesk, following the process set out in the SAIL Incident Management policy (see references). The helpdesk can be accessed via helpdesk@chi.swan.ac.uk or https://jira.hiru.swan.ac.uk/servicedesk.

1.2 Retention Schedule

The table below sets out the type of documentation and data that is retained for specific SAIL purposes and the length of retention. In each case, a justification for this retention has been included.

Operation	Data type	Data location	Retention Period	Retention purpose
SAIL user management	Evidence of being a 'safe' researcher - CVs	Security 3	Date of approval + 1 month (maximum)	Once a researcher has been approved as a "safe researcher", there is no further requirement to hold their CVs. The evidence of approval by the director is logged and serves as evidence of the process being followed. CVs are never re-reviewed after this has taken place. SAIL will hold these for no longer than 1 month after the approval is granted (to account for system/personal error).
SAIL user management	Evidence of user training records (safe researcher)	Security 3	Until account is disabled + 1 year	SAIL user training is a mandatory requirement for use of SAIL data. This data must be retained for the lifetime of the user's access to SAIL to demonstrate this is being met
SAIL user management	Security 3 accounts and login usernames	Security 3	Until account is disabled + 6 years	SAIL user accounts on Security 3 are automatically disabled once a user's projects or safe researcher training have expired. SAIL retains these accounts on the system beyond this period for the purposes of any potential data access audit requirements that may arise. This also prevents re-issuing of old usernames to new users within a short timeframe and avoids complications during audits.
SAIL user management	Data access agreements	Security 3	Until account is disabled + 6 years	Data access agreements are evidence of individual liability and must be retained in the event that user misconduct needs to be followed up after they have stopped using the service.
SAIL Project Development	IGRP forms	P drive; IGRP System	Project duration + 6 years	Retention in line with the JISC guidance – research business development (records documenting the formation and management of partnerships and other collaborative arrangements to undertake research)
SAIL Project Development	Data sharing agreements	Contracts doc store?	Lifetime of data sharing arrangement + 6 years	Retention in line with the JISC guidance – research business development (records documenting the formation and management of partnerships and other collaborative arrangements to undertake research)
SAIL Project Development	Scoping forms (resulting in project)	Security 3	Project duration + 6 years	In alignment with *Contracts* retention (see below), as scoping forms relating to projects are appended to contracts.
SAIL Project Development	Scoping forms (not resulting in project)	Security 3	Last contact + 6 months	SAIL recognises that the scoping process can be subject to delay whilst project initiators confirm specific details. SAIL will keep this document for as long as there is active discussion around the proposed project, but will delete the form if 6 months passes without any further development. Past this point, projects will need to start the scoping process again from scratch.
SAIL Project Development	Contracts	Contracts doc store?	Contract length + 6 years	Retention in line with the JISC guidance – research business development (records documenting the formation and management of partnerships and other collaborative arrangements to undertake research)

SAIL Research	SAIL research data (anonymised)	SAIL Databank	Indefinite	Anonymised data is not required to set a retention period. SAIL as standard does not delete anonymised data. Any deletion of anonymised data must be specifically requested by the data provider or detailed within the relevant data sharing agreement.
SAIL Research	SAIL research data (identifiable)	N/A	Period to be agreed in data sharing agreement	Retention period would be set out in the data sharing agreement. At present and as standard, SAIL does not hold identifiable research data.

1.3 Data deletion process

Deletion arrangements for the data will depend on the file storage arrangements for each dataset.

Digital files

Where possible, automation will be utilised to alert the teams responsible for digital files when deletion is necessary. SAIL utilises a range of digital systems for file storage which, at present, do not support fully automated deletion scheduling.

The SAIL Data Governance and SAIL Business teams will be responsible for reviewing the systems under their ownership for files which require deletion.

SAIL Databank

Data deletion methods, where necessary, will be determined by the data provider's requirements (as set out in the Data Sharing Agreement). Management of these data deletion arrangement will be the responsibility of the SAIL Technical team. Anonymised research data is **NOT** subject to data deletion requests.

Paper records

SAIL works to minimise paper records where possible. Documentation **will be held** digitally as a default, although some historic documents may still be held on paper. These documents will be destroyed (shredded securely with an ISO27001 compliant device).

1.4 Audit of data retention

The application of this data retention schedule will be subject to an annual sample audit. These audits will take the following form:

- Audit team will be comprised of members of the Information Security team. SAIL staff with access to relevant systems will be required to support the audits.
- Sample to include (where possible) at least one example from each data type.
- Evidence of non-conformance to the policy will be raised on the DSB NCPAR and may prompt a further audit outside of the scheduled bi-annual audit programme.
- Audits will generate an audit report to be prepared and held by the Information Security team
- The DSB Internal Audit committee will be responsible for ensuring this process takes place.

2. SAIL DATA RETENTION - ROLES AND RESPONSIBILITIES.

Role	Functional Responsibilities.
Audit and Compliance Manager	Responsible for ownership of the Data Retention policy and ensuring content remains up to date. Responsible for resourcing data retention audits (as set out above)
SAIL Technical team	Responsible for ensuring that data retention automation measures (around deletion) are established. Responsible for addressing any identified faults with data retention automation measures and implementing necessary fixes. Responsible for managing retention actions relating to data on the SAIL Databank
SAIL Data Governance team SAIL Business team	Responsible for ensuring that systems under their management are retained data in line with the stated arrangements in this policy.

DSB Internal Audit Committee	Responsible for ensuring that data retention audit schedule is carried out Responsible for ensuring that actions resulting from data retention audits are followed up on and tracked through the DSB NCPAR document.

3. SAIL DATA RETENTION - COMPLIANCE.

Any staff subject to this policy who intentionally fail to comply with the provisions as set out above shall be subject to appropriate management response. This may include disciplinary action in accordance with the Swansea University Disciplinary Code and Procedures.

SAIL Information Security policies, standards, procedures and guidelines shall comply with legal, regulatory and statutory requirements.

A. DOCUMENT MANAGEMENT.

A.1 AUTHORISATION.

NAME	TITLE
David V Ford	Co-Director / Professor SAIL Programme
Sharon Heys	Head of Legislation and Due Diligence

A.2 DISTRIBUTION.

NAME	TITLE
David V Ford	Co-Director / Professor SAIL Programme
Sharon Heys	Head of Legislation and Due Diligence
All SAIL Staff	(Available via Confluence and OwnCloud).
Policy will be publicly available via the website	

A.3 REFERENCES.

DOCUMENT
JISC guidance (https://www.jisc.ac.uk/guides/records-retention-management)
SAIL-POL-012 – Information Security Incident Management policy

A.4 DOCUMENT HISTORY.

VERSION	DATE	AUTHOR	DESCRIPTION	APPROVED BY
0.1	16/02/2023	Rob Garlick	Initial draft version	Rob Garlick
0.2	27/02/2023	Sharon Heys	Internally reviewed with additional comments	Rob Garlick