AUSTRALIAN ACCESS FEDERATION

NCRIS National Research Infrastructure for Australia An Australian Government Initiative

AAF is enabled by NCRIS

[PDK03]

Policy on the Processing of Personal Information

Key questions to inform policy development

- What are the purposes for processing personal information? Are they limited to the management, operation and security of the Collaboration?
- Who has access to personal information and why? How is this controlled?
- Is personal information properly protected?
- Does the User have access to their personal data?

*Delete this box after completing the policy.

1 Introduction and Purpose

1.1 Objectives

This Policy defines the protocols all Service Providers must abide by to ensure the protection and lawful processing of personal information related to Users collected due to their use of Collaboration Services offered by the Collaboration.

1.2 Scope

This Policy applies to all User's personal information that is processed due to their use of Collaboration Services.

This Policy does not apply to personal information relating to third parties included in datasets provided by the User or the research community they belong to as part of their research activity within the Collaboration. Examples of such information includes medical datasets which may contain personal information.

Where local policies and processes of Service Providers conflict with this Policy, Collaboration Policies take precedence as it pertains to the management, operation and security of the Collaboration.

1.3 Legislative Compliance

In implementing this Policy, the Collaboration and its Service Providers will ensure compliance with legislative instruments, including state, national and international jurisdictions relevant to the operation of the Collaboration.

1.4 Definitions

Personal information: Any information relating to an identified or reasonably identifiable natural person. Examples of personal information include User registration, credential identifiers and usage, and the monitoring, audit of records.

Processing (processed): Any operation, or set of operations, including collection and storage which is performed upon personal information.

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2) and Grant Agreement No. 653965 (AARC). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

Additional terms are defined in the Top-Level Collaboration Policy.[1]

2 Obligations of Service Providers

By agreeing to abide by Collaboration Policies, Service Providers must declare:

1. They have read, understood and will abide by the Principles of Personal Information Processing set out in this Policy, and
2. Their acknowledgement that failure to abide by these Principles, or other relevant Collaboration Policies, may result in the exclusion from the Collaboration; and if such failure is reasonably suspected by Collaboration Management to be the result of an unlawful information disclosure, they may be reported to relevant legal authorities.

3 Principles of Personal Information Processing

1. The User whose person information is being processed shall be treated fairly and in an open and transparent manner.
2. Personal information of Users (hereafter, personal information) shall be processed only for those administrative, operational, accounting, monitoring and security purposes that are necessary for the safe and reliable operation of Collaboration Services, without prejudice to the User's rights under relevant laws.
3. Processing of personal information shall be adequate, relevant and not excessive in relation to the purposes for which it is processed.
4. Personal information shall be accurate, and where necessary, kept up to date. Where personal information is found to be inaccurate or incomplete, having regard to the purpose for which it is processed, it shall be rectified or purged.
5. Personal information processed for the purposes listed in clause 3.2 of this Policy shall not be kept for longer than the period defined in the relevant Collaboration Policy governing the type of personal information being processed (e.g. registration, monitoring, accounting or security), and by default shall be anonymised or purged after the period specified in in the Collaboration Privacy Policy.
6. Appropriate technical and organisational measures shall be taken against unauthorised disclosure or processing of personal information and against accidental loss, destruction of, or damage to personal information. At a minimum, Service Providers must:
    a. Restrict access to stored personal information under their control to appropriate, authorised individuals;
    b. Transmit personal information by network or other means in a manner to prevent disclosure to unauthorised individuals;
    c. Not disclose personal information unless in accordance with the Principles outlined in this Policy;
    d. Appoint at least one Privacy Officer with appropriate training and publish to the Collaboration a single point of contact for the Privacy Officer to which Users and other Service Providers can report suspected breaches of this Policy;

[1] <Link to PDK01>

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2) and Grant Agreement No. 653965 (AARC). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

e. Respond to suspected breaches of this Policy promptly and effectively and take the appropriate action where a breach is found to have occurred, including making any necessary disclosures as required by law;
f. Perform periodic audits of compliance to this Policy and make available the results of such audits to Collaboration Management other Service Providers upon their request.

7. Each Collaboration Service interface provided to the User must present, in a clear and accessible way, a Privacy Policy containing the following elements:
    a. The name and contact details of the Collaboration Service Provider processing personal information;
    b. A description of the personal information being processed;
    c. The purpose(s) of processing personal information;
    d. An explanation of the rights of the User to:
        i. Obtain a copy of the personal information being stored by the Service Provider without undue delay;
        ii. Request that any personal information relating to them which is shown to be incomplete or inaccurate be rectified; and
        iii. Request on compelling legitimate grounds that the processing of their personal information should cease.
    e. The contact details of the Service Provider's Privacy Officer to which the User should direct requests in relation to their rights in clause 7.d of the Principles outlined in this Policy;
    f. The retention period of the personal information processed;
    g. Reference to this policy; and
    h. Any other elements that may be required by law.
8. Personal information may only be transferred or otherwise shared with individuals or organisations where the recipient:
    a. Meets the requirements of the Australian Privacy Act 1988 (Cth) Australian Privacy Principles as it pertains to the transfer of personal information offshore and to third parties and;
    b. Has agreed to be bound by the Collaboration Policies; or
    c. Is part of a recognised Computer Incident Response Team framework and as part of an incident investigation to prevent active or suspected misuse of Collaboration Services; or
    d. Presents an appropriately enforced legal request.

4 Associated Documents

4.1 Collaboration Policies

- Top-Level Collaboration Policy [PDK01]
- Privacy Policy [PDK02]
- Acceptable Use Policy [PDK04]
- Acceptable Authentication Assurance Policy [PDK05]
- Community Membership Management Policy [PDK06]
- Service Operations Security Agreement [PDK07]
- Security Incident Response Procedure [PDK08]

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2) and Grant Agreement No. 653965 (AARC). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

4.2 Relevant Legislation, Standards & Frameworks

[Include all legislation, standards, and frameworks relevant to the Collaboration, highlighting their alignment with Australian laws as well as applicable international standards and regulations].

- *Privacy Act (1988)* (Cth) (Australian Privacy Principles)
- *Other relevant international standards and legislation (e.g. General Data Protection Regulation, FAIR and CARE Principles)*

Version Control

Document Control				
Document Approved:			**Date Effective:**	
Last Review Date:			**Next Review Date:**	
Version Control				
Version	**Author**	**Summary of Changes**		**Date**
0.1	AAF	Review and alignment of language and legislative requirements. Introduction of clause 7(h) to ensure Service Providers comply with legislation that may apply to their context. Refinement of context statements. Corrected attributions. Updated disclaimer.		March 2025

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2) and Grant Agreement No. 653965 (AARC). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).

Schedule 1: Required Registration Data

The Registry must store at least:

- Registration data, including personal information of the User
- attributes assigned to members
- <Add or delete lines as required>

The Registration data for a User comprises verified information on at least:

- family name(s)
- given name(s)
- the employing organisation name and address
- any applicable Sponsor identity
- a professional (organisational) email address
- unique and non-reassigned identifier(s) of the User and the source of authority of each identifier
- <Add or delete lines as required>

and is recommended to contain:

- a professional (organisational) contact telephone number so as to inform the User promptly during the investigation of security incidents and of lifecycle events
- other contact information, as voluntarily provided and maintained by the User.

Other Sources / Attribution / Acknowledgements: The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2) and Grant Agreement No. 653965 (AARC). Adapted by the Trust and Identity Pathfinder Policy Working Group coordinated by the AAF, comprised of members from Australian national research infrastructure, and enabled by funding through the Australian Government's National Collaborative Research Infrastructure Strategy (NCRIS).