Questions to ask yourself when defining this policy:

- Purpose of processing personal information?
- Who has access to this information and why?
- Is the information properly protected?
- Does the user have access to their personal information?

**delete this box after completing the policy.*

Policy on the Processing of Personal Information

This policy is effective from <insert date>.

Introduction

This policy ensures that data collected as a result of the use of the Collaboration is processed fairly and lawfully by Collaboration participants. Some of this data, for example that relating to user registration, monitoring and accounting contains “personal information” as defined by the Privacy Act 1988 (see https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information) . The collection and processing of personal information is subject to restrictions aimed at protecting the privacy of individuals.

Definitions

Definitions that are relevant to more than one policy are contained in the Top Level Collaboration Policy. Definitions that are relevant only to this policy are included here.

Personal Information - Any information relating to an identified or identifiable natural person.
Processing (Processed) - Any operation or set of operations, including collection and storage, which is performed upon Personal

Scope

This policy covers Personal information that is Processed as a prerequisite for or as a result of an End User’s use of Collaboration services. Examples of such Personal

Information include registration information, credential identifiers and usage, accounting, security and monitoring records.
This policy does not cover Personal Information relating to third parties included in datasets provided by the End User or the research community to which they belong as part of their research activity. Examples of such data are medical datasets which may contain Personal Information.

Policy

By their activity in the Collaboration, Service Providers:

1. Declare that they have read, understood and will abide by the Principles of Personal Information Processing as set out below.
2. Declare their acknowledgment that failure to abide by these Principles may result in exclusion from the Collaboration, and that if such failure is thought to be the result of an unlawful act or results in unlawful information disclosure, they may be reported to the relevant legal authorities.

Principles of personal information processing

I. The End User whose Personal Information is being Processed shall be treated fairly and in an open and transparent manner.
II. Personal Information of End Users (hereinafter “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 End Users’ rights under the relevant laws.
III. Processing of Personal Information shall be adequate, relevant and not excessive in relation to the purposes for which they are Processed.
IV. Personal Information shall be accurate and, where necessary, kept up to date. Where Personal Data are found to be inaccurate or incomplete, having regard to the purposes for which they are Processed, they shall be rectified or purged.
V. Personal Information Processed for the purposes listed under paragraph ii above shall not be kept for longer than the period defined in a relevant service policy governing the type of Personal Information record being Processed (e.g. registration, monitoring or accounting) and by default shall be anonymised or purged after a period specified in the Privacy Policy.

Policy Development Kit was reviewed by the AAF Trust and Identity Pathfinder Policy Working Group, by and for Australian national research infrastructure, enabled by NCRIS.

VI. Appropriate technical and organisational measures shall be taken against unauthorised disclosure or Processing of Personal Information and against accidental loss or destruction of, or damage to, Personal Information. As a minimum, Collaboration Service Providers shall:

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 these Principles of Personal Information Processing;
D. Appoint at least one Data Protection Officer (DPO) with appropriate training and publish to the Collaboration a single contact point for the DPO to which End Users or other Collaboration Participants can report suspected breaches of this policy;
E. Respond to suspected breaches of this Policy promptly and effectively and take the appropriate action where a breach is found to have occurred;
F. Perform periodic audits of compliance to this Policy and make available the results of such audits to other Collaboration Participants upon their request.

VII. Each Collaboration service interface provided for the End User must provide, in a visible and accessible way, a Privacy Policy containing the following elements:

1. Name and contact details of the Collaboration Participant Processing Personal Information;
2. Description of Personal Information being Processed;
3. Purpose or purposes of Processing of Personal Information;
4. Explanation of the rights of the End User to:
    a) Obtain a copy of their Personal Information being stored by the Participant without undue delay;
    b) Request that any Personal Information relating to them which is shown to be incomplete or inaccurate be rectified;
    c) Request that on compelling legitimate grounds Processing of their Personal Information should cease;
5. The contact details of the Collaboration Participant's DPO to which the End User should direct requests in relation to their rights above;
6. Retention period of the Personal Information Processed;
7. Reference to this Policy.

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Policy Development Kit was reviewed by the AAF Trust and Identity Pathfinder Policy Working Group, by and for Australian national research infrastructure, enabled by NCRIS.

VIII. Personal Information may only be transferred to or otherwise shared with individuals or organisations where the recipient:

1. has agreed to be bound by this Policy and the set of common Collaboration policies, or
2. 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
3. presents an appropriately enforced legal request.

 The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Policy Development Kit was reviewed by the AAF Trust and Identity Pathfinder Policy Working Group, by and for Australian national research infrastructure, enabled by NCRIS.