

[PDK04]

Acceptable Use Policy

Key questions to inform policy development:

- What is your Collaboration's aim and purpose?
- Does the Collaboration guarantee any availability of your Services to your users?
- Do Users need to cite the Collaboration or its Services in published works?
- Can infrastructure be used for commercial purposes?
- Do Collaboration Service Providers have specific clauses required for use?
- Does the Collaboration wish to prevent the use of specific technology when Users access Services?
- Do Communities or Service Providers have specific standards regarding the use of artificial intelligence in research applications?

When using the baseline AUP text below, curly brackets "{}" (coloured blue) indicate text which should be replaced as appropriate to the community, agency or infrastructure presenting the AUP to the user. Angle brackets "< >" (coloured green) indicate text which is optional and should be deleted or replaced as indicated. Other text should not be changed.

*Delete this box after completing the policy

1 Introduction and Purpose

1.1 Objective

This Policy contains the Acceptable Use Policy (AUP) and Conditions of Use baseline document for the Collaboration.

1.2 Scope

The Acceptable Use Policy applies to all registered Users within the Collaboration.

1.3 Implementation

This Policy must be implemented in accordance with Collaboration Policies, particularly the Top-Level Collaboration Policy.¹

1.4 Definitions

Terms are defined in the Top-Level Collaboration Policy.²

¹ Refer to <link to Collaboration Policies>

² <Link to PDK01>

2 Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use (AUP) defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and Services as granted by {Collaboration Name, Service Provider Name, or Community} for the aims and purpose of {describe the stated goals and policies governing the intended use}.

<To further define and limit what constitutes acceptable use, the Collaboration, Service Provider or Community may optionally add additional information, rules or conditions, or references thereto, here or at the placeholder below. These additions must not conflict with the clauses 1-10 below, whose wording and numbering must not be changed.>

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other Users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.
4. You shall protect your access credentials (e.g. passwords, private keys or multi-factor tokens); no intentional sharing is permitted.
5. You shall keep your registered information correct and up to date.
6. You shall promptly report known or suspected security breaches, credential compromise, or misuse to the Security Contact stated below; and report any compromised credentials to the relevant issuing authorities.
7. Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.
8. Your personal data will be processed in accordance with the privacy statements referenced below.
9. Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.
10. If you violate these rules, you may be liable for the consequences, which may include your account being suspended and a report being made to your home organisation or to law enforcement.
11. <Insert additional numbered clauses here.>

[If one AUP for the Collaboration, for example:] <Service Provider A> Acceptable Use Terms

12. <Insert additional numbered clauses here.>

Note

If implementing one AUP with multiple subsections, AAF recommends listing the relevant contact details and privacy documentation pertinent to the Service Provider or Community outlined below with the AUP Terms for each entity.

*Delete this box after completing the policy.

The administrative contact for this AUP is: {email address for the Collaboration, Service Provider or Community Name}

The Security Contact for this AUP is: {email address for the Collaboration or Service Provider Security Contact}

The Collaboration Privacy Policy is located at: {URL}

The Collaboration Policy on the Processing of Personal Information is located at: {URL}

Other applicable Privacy Policies are located at: <URLs>

Applicable service-level agreements are located at: <URLs>

Version Control

| Document Control | | | |
|--------------------|--------|---|------------|
| Document Approved: | | Date Effective: | |
| Last Review Date: | | Next Review Date: | |
| Version Control | | | |
| Version | Author | Summary of Changes | Date |
| 1.5 | AAF | Review and alignment of language. Refinement of context statements. Corrected attributions. Updated disclaimer. | March 2025 |
| | | | |
| | | | |
| | | | |

AAF NRI Policy Development Kit – Acceptable Use Policy [PDK04]

© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

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). Based on "The WISE Baseline Acceptable Use Policy and Conditions of Use" provided by Members of the WISE Community SCI Working Group, and used under CC BY-NC-SA 4.0. 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).

This document is provided as guidance only. Each organisation or Collaboration must consider its own unique context, legislative obligations, and trust and identity requirements to complete and implement the Trust and Identity Policy Development Kit. AAF and other national research infrastructure members of the Policy Working Group, are not liable for any loss or damage, from any implementation or action taken to implement this Policy.