

This Privacy Policy sets out the way in which Queensland Cyber Infrastructure Foundation Ltd ACN 094 639 406 (we, us, our) collects, uses, stores and discloses your Personal Information.

As circumstances or the law change, we will update our Privacy Policy and post the updated policy on our Website. To ensure you are aware of any changes, you should review our Privacy Policy each time you provide us with Personal Information.

QCIF has adopted the 13 Australian Privacy Principles (APP) from Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Act 2012, which amends the Privacy Act 1988 (the Privacy Act). The APPs came into effect on the 12th of March 2014.

Consent

By providing us with Personal Information, you consent to us collecting, using and disclosing that information (within and outside Australia) in accordance with our Privacy Policy.

Interpretation

For the purposes of our Privacy Policy:

- **Personal Information** has the same meaning as under the Privacy Act and includes Sensitive Information.
- **Privacy Act** means the Privacy Act 1988 (Cth) including the Australian Privacy Principles and any amendments to the Privacy Act or Australian Privacy Principles from time to time.
- **Privacy Policy** means this document as amended from time to time. Related Entities has the same meaning as under the Corporations Act 2001 (Cth) and includes our members, associate members and co-investors.
Sensitive Information has the same meaning as under the Privacy Act.
- **Services** means the services provided by us, including facilitating collaborative research through the provision and utilisation of Research Tools.
- **Research Tools** means the information technology and internet-based research tools provided by us including, without limitation,

ReDBox, SeeVogh, Quadrant, QRIScloud and High Performance Computing services.

- **Website** means all websites operated or utilised by us, including www.qcif.edu.au and www.griscloud.org.au.

The meaning of any general language is not restricted by any accompanying example and the words 'includes', 'including', 'such as', 'for example' or similar words are not words of limitation.

What Personal Information do we collect and why do we need it?

To provide our Services, we need to collect Personal Information. If we do not do so or if the information is incomplete or inaccurate, we may not be able to provide our Services or those Services may be compromised.

Depending on the nature of the Services we provide to you or a University or other entity you represent, the Personal Information we collect may include:

- your name, email address, telephone numbers and address;
- your employer and position description;
- academic qualifications and transcripts;
- user names and passwords; and
- about how you use our Services.

This is not an exhaustive list and additional information may be collected as part of a user authentication process for our Services.

How do we collect the Personal Information?

General

We aim to collect Personal Information directly from you. Generally this occurs when you complete a form, make inquiries or utilise our Services. We may also collect Personal Information:

- through our Website and Research Tools;

- from third parties, for example, through another subscriber or researcher;
- from publicly available sources of information;
- from our records of how you use our Services; or
- when we are required to do so by law.

Personal Information about third parties

If at any time you supply Personal Information to us about any other person (for example, another researcher or user), you represent and we accept that information solely on the basis that you are authorised to do so and that the relevant person has consented to the disclosure to us.

How do we use your Personal Information?

General

In addition to any other purposes set out in this Privacy Policy, we use the Personal Information we collect to:

- verify your identity or conduct appropriate checks in connection with your use of the Services;
- process your inquiries;
- provide and administer our Services or services of third parties;
- comply with our contractual and other legal obligations (including as required by laws which apply to us);
- to monitor use, infrastructure quality and performance and operate, maintain, develop, test and upgrade our systems and infrastructure;
- to your authorised representatives or advisers, or when you ask us to do so;
- develop and improve our Services;
- protect and enforce our legal rights; and
- protect and defend our, or our employees, users and clients' rights or property including against fraudulent or unlawful use of our Website or Research Tools.

Marketing and Surveys

We may use and disclose your Personal Information (except Sensitive Information) to provide you with information on offers, products and

services offered by us or our Related Entities or to conduct surveys to improve our Services.

If at any time you no longer wish to receive any additional marketing or survey material from us or do not want your information disclosed for direct marketing or survey purposes, contact our Privacy Officer and we will remove your details from our marketing database.

Disclosing Personal Information

We may disclose your Personal Information to third parties in certain circumstances including:

- if you agree to the disclosure;
- for the purpose for which it was collected, for example, to provide you with Services;
- where you would reasonably be expected to consent to information of that kind being passed to a third party;
- where disclosure is required or permitted by law, by court order or to investigate suspected fraud or other unlawful activity;
- where it is required to be disclosed for audit purposes;
- to our Related Entities;
- if disclosure will prevent or lessen a serious or imminent threat to someone's life or health;
- if applicable, fraud-checking agencies; or
- where it is reasonably necessary for the enforcement of the criminal law, a law imposing a pecuniary penalty or for the protection of public revenue.

Considerations when you send information to us electronically

While we do all we reasonably can to protect your Personal Information from misuse, loss, unauthorised access, modification or disclosure, including investing in security software, no data transfer over the internet is 100% secure. The open nature of the internet is such that information exchanged via the internet may be accessed and used by people other than those for whom the data is intended. If you send us

any information, including (without limitation) Personal Information, it is sent at your own risk.

If you access another website from our Website (or from a website through which we offer the Services), you do so and provide Personal Information in accordance with the terms and conditions under which the provider of that website operates.

Storage and retention of Personal Information

We endeavour to keep our information systems and files secured from unauthorised access. Our procedures to securely store Personal Information include electronic and physical security measures, staff training and use of password protection software.

When the Personal Information we collect is no longer required, we will remove or de-identify the Personal Information as soon as reasonably possible. We may, however, retain Personal Information for as long as is necessary to comply with any applicable law, for the prevention of fraud, for insurance and governance purposes, in our IT back-up, for the collection of any monies owed and to resolve disputes.

How you can update, correct, or delete your Personal Information

You may request access to your Personal Information or correct any inaccurate or out of date information by contacting our Privacy Officer using the details below. You may request the source of any information we collect from a third party. We will provide this at no cost, unless under the Privacy Act or other law there is a reason for this information being withheld.

If there is a reason under the Privacy Act or other law for us not to provide you with information, we will give you a written notice of refusal setting out the reasons for the refusal (except to the extent it would be unreasonable or unlawful to do so) and advise you of the mechanisms available to you to complain about the refusal.

Dealing with a complaint

If you make a complaint about a privacy matter, our Privacy Officer will respond as soon as possible (but within 14 days) and advise you who in our company will have responsibility for investigating and managing your complaint.

We will try to resolve your complaint within 30 days of receiving it. If this is not possible, we will contact you and provide you with an estimate of the time it will take to investigate and manage the complaint.

Contact information

Our Privacy Officer

You should also contact us directly or contact our Privacy Officer if:

- you believe someone has gained access to your Personal Information;
- you think that your account number, username or password have been compromised (in which case you should also immediately change your password); or
- you believe we have breached our privacy obligations or your privacy rights in any way;
- you would like further information on our Privacy Policy; or
- you have any concerns over the protection of the Personal Information you have given to us or that we have collected from others

Our Privacy Officer can be contacted by sending an email to support@griscloud.org.au, with Attention: Privacy Officer in the subject field.

Privacy Commissioner

More information about your rights and our obligations in respect to privacy and information on making a privacy complaint are available from the Office of the Australian Information Commissioner at:

- Website: www.oaic.gov.au
- Post: GPO Box 5218 Sydney NSW 2001
- Email: enquiries@oaic.gov.au