

PRACE Acceptable Use Policy

8 September 2014



General Use Policy

1. Introduction

1.1. This Acceptable Use Policy (“AUP”) applies to all Users of the PRACE infrastructure. This AUP is in addition to any policies or conditions which may be imposed by the Resource Providers.

1.2. PRACE may make any reasonable changes to this AUP at any time and will inform the user. If the User does not accept these changes, it may cease to use the Resources at any time.

1.3. For the purposes of this AUP, the following terms will have the following meanings:

- The PRACE infrastructure means the facilities and services, to which PRACE awards access, in particular the Tier-0 systems provided by the Hosting Members.
- Resources are all ICT facilities which are provided as part of the PRACE infrastructure
- The User means such individuals who have been approved to use the Resources;
- Resource Providers means those PRACE Members or the AISBL who provide Resources in accordance with the terms of the resource allocation procedure;
- Malicious Software means computer virus, Trojan, worm, logic bomb or other harmful material;
- Project means the research work carried out by a group of users;
- The Registrar means the body or bodies awarding access to the Resources.

2. General Use

2.1 The User will have regard to the principles which require that PRACE acts exclusively for peaceful purposes and conduct its activities in an ethical manner.

2.2 The User agrees that logged information, including information provided for registration purposes, is used for administrative, operational, accounting, monitoring and security purposes only. This information may be disclosed, via secured mechanisms, only for the same purposes and only as far as necessary to other organizations cooperating with the Resource Providers. Although efforts are made to maintain confidentiality, no guarantees are given.

2.3 The User will inform the Registrar and the Resource Providers if there are any changes to its contact information.

2.4 The User agrees to use the resources only to perform work, or transmit or store data consistent with the stated goals and policies and conditions of use as defined by the Registrar.

2.5 The right to use Resources is strictly personal and may not be transferred to any other third party. The Registrar and Resource Providers are entitled to regulate, suspend or terminate the User access, within their domain of authority, and the User shall immediately comply with their instructions. The rights to use Resources will terminate when the period of allocation comes to an end.

2.6 The User recognises that the use of Resources by nationals of certain countries may be restricted by policies laid down by the Registrar or the Resource Providers.

2.7 The User will respect all proprietary rights (which may also be considered intellectual property) belonging to the Resource Providers, including any copyright and licences.

2.8 The User will keep confidential all information which is obtained through the use of the Resources which it may reasonably be expected to know is confidential or sensitive.

2.9 The Resource Providers reserve the right to manage the usage of Resources in order to ensure full optimisation of the Resources, even if this may cause some limitation of usage for the User or changes to the Resources.

2.10 The User will not transport any data, which it may reasonably be expected to know is confidential or sensitive, e.g. credentials on IT equipment without adequate protection (such as encryption) in place.

2.11 The use of Resources is at the risk of the User. The Resource Providers don't make any guarantee as to their availability or their suitability for purpose.

2.12 Resource Providers and Registrar will not be liable for any damages suffered by the User.

2.13 The User will exercise all reasonable care when accessing Resources.

3. Unacceptable Use

3.1 The User will not use Resources for any unacceptable purposes. Unacceptable purposes include but are not limited to:

- 3.1.1 any activity which is illegal under local, national or international law;
- 3.1.2 any attempt to breach or circumvent any administrative or security controls;
- 3.1.3 any creation, storage, use or transmission of data which is in breach of any copyright or licence;
- 3.1.4 any activity which purposely causes material or moral damage to the Resource Providers, or which causes loss of operational efficiency, or loss or corruption of Resources;
- 3.1.5 any activity which interferes with the use of Resources by other users;
- 3.1.6 any activity which compromises the privacy of other user;
- 3.1.7 any activity which may lead to the use or distribution of Malicious Software.

4. Security

4.1 It is the responsibility of the User to protect the details of its user account and access credentials.

4.2 The User will not divulge its access credentials.

4.3 The User will not use any other user's credentials to access the Resources.

4.4 The User will take all reasonable steps necessary to protect the security of personal computers, laptops and workstations, from which he accesses the Resources, against unauthorised access. Recommended security measures include the use of password-

protected screensavers and locking and/or shutting down terminals when left unattended or not in use.

4.5 The User will not use any computer applications which jeopardise the functioning of Resources. The Resource providers will notify the User concerned who will be required to take all steps necessary to detect the cause and prevent re-occurrence. The Resource providers have the right to suspend the User's access to the Resources if necessary and to prohibit any computer application which, in its reasonable opinion, poses a security threat.

4.6 The User agrees to comply on use with any special conditions which may apply to specific software installed on the Resources.

4.7 The User will report immediately to the Resource Providers if it becomes aware of any unauthorised use of its user account, or if it knows or suspects that there has been a breach of security or misuse of the Resources. Failure to do so will enable the Resource Providers to terminate the User's use of Resources.

5. Liabilities and Sanctions

5.1 The User will be liable for any damages resulting from the infringement of this AUP or any other policies or conditions imposed by the Resource Providers and which have been communicated to the User.

5.2 Any infringement or potential infringement will be notified to the User in writing. If the infringement persists and/or further infringements are detected and/or where it is justified by the seriousness of the infringement, the Resource Providers may withdraw access rights to Resources and/or initiate disciplinary proceedings and/or legal proceedings against the User.

Particular Use Policy

(to be provided by the resource provider)

Name and surname of the PI:

Signature of the PI:

Date: