RESEARCH USE OF INFORMATION TECHNOLOGY INFRASTRUCTURE POLICY

Section	Information Technology Services
Contact	Information Technology Services
Last Review	September 2007
Next Review	September 2009
Approval	

Purpose:

The purpose of this policy is to ensure:
- the efficient and effective use of the University's infrastructure;
- that competing users of the infrastructure are considered;
- that University policies, particularly the Policy on Research Practice which includes the Code of Ethical Conduct for Research, Teaching and Evaluations involving Human Participants are implemented; and
- that issues of safety, scope, privacy, copyright and liability are identified and managed.

Definitions:

"Information Technology Infrastructure" means telecommunications and data networking infrastructure and network services.

Policy:

Any use of the University's Information Technology Infrastructure for research purposes will only be for authorised purposes.

Research using Information Technology Infrastructure must be approved in advance of the research being undertaken.

Audience:

All users of the Information Technology Infrastructure for research purposes, including staff and students.

Relevant legislation:

- Privacy Act 1993
- Copyright Act 1994
- Films, Videos, and Publications Classification Act 1993

Legal compliance:

Privacy Act 1993
The Privacy Act 1993 governs the collection and use of information held by the University for the purposes of the University's management and administration. Personal information held for these purposes will not be used for other

purposes. Release of personal information otherwise than in accordance with the terms of the Privacy Act is strictly prohibited.

Copyright Act 1994
Under the Copyright Act 1994 it is illegal to make or distribute copyright material without specific authorisation from the copyright owner. The University absolutely forbids the use of its computer and network facilities for a purpose, which constitutes an infringement of copyright.
- No material is to be used without the written permission of the copyright owner.
- Copyright information is provided at the following intranet address: http://www.copyright.co.nz/

Films, Videos, and Publications Classification Act 1993
- The Films, Videos, and Publications Classification Act 1993 classifies (ie. censors) publications. Objectionable material in particular is banned - it is illegal to possess, own, sell, hire, give or buy an objectionable publication.
- Something is "objectionable" if "it describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good" (section 3 of the Act).

Researches must ensure that in using the University's Information Technology Infrastructure they do not breach the requirements of this Act.

Related documents:

Policy on Research Practice
Code of Ethical Conduct for Research, Teaching and Evaluations involving Human Participants
Data Network Policy
Telecommunications Policy
Use and Access to Information Technology Systems Policy

Related procedures:

Staff and students of the University are entitled to use the University's Information Technology Infrastructure only for authorised University purposes. Procedures outlining how such authorisation is obtained are detailed below:

1   Approval Process

   1.1   The use of the Information Technology Infrastructure for research purposes requires the explicit permission from the office of the Chief Information Officer.

   1.2   Applications for approval should be sent to the Chief Information Officer and must include the following documentation submitted to the University's research-authorising bodies. Documentation should include:
      a. all relevant documentation submitted to the University's research-authorising bodies by that researcher, including subsequent authorisations;
      b. a full description of the likely scope and impact of the proposed research on the University's Information Technology Infrastructure;
      c. the proposed timeframes for use of the Information Technology Infrastructure;
      d. appropriate details to allow relevant charges for costs to be applied - ie. Data volumes, access requirements, service levels, hosting requirements, security, issues, funding source etc; and
      e. sufficient information to ascertain whether sensitive content or materials are likely to be involved as part of the research, including plans to remove the risk of accidental exposure to other parties.

1.3   Permission will be withheld if:
   a.   the proposed research has not been approved by other relevant research-authorising bodies of the University;
   b.   the proposed research impacts negatively on the effective delivery of routine services to the University community or on the wider community of users of that infrastructure; and
   c.   the scale or scope of the research is undefined in terms of its potential impact on the University's Information Technology Infrastructure.

Responsibilities of the researcher

The researcher is responsible for:

   a.   all costs associated with the use of a service provided;
   b.   ensuring that a secure backup is kept of all data that is part of the research and that a backup alternative exists in the event of failure of a piece of technology; and
   c.   ensuring that the use has been checked against the researcher's intended purpose prior to the research activity commencing.

1.1   Where Information Technology Infrastructure is being used by a researcher in such a way that the content or subject matter of the use is sensitive or likely to raise questions related to inappropriate use of Information Technology Infrastructure, the researcher must take appropriate steps to ensure that:
   a.   none of their colleagues or any other staff members, students or other people are exposed to material that may cause offence; and
   b.   there is no breach of any laws regarding the viewing, use or publication of materials. Massey University takes no responsibility for any emotional or mental harm resulting from researchers using the University's Information Technology Infrastructure for their own research needs.

1.2   Researchers are responsible for the destruction of recorded materials relating to their research work. In particular, if sensitive or confidential material is recorded on any Information Technology Infrastructure, the destruction process should include complete data wipe procedures.[1]

1.3   The University's network, systems and telecommunications environment provides services that are designed to operate on a 7 x 24 basis. However, outside of the University's business hours (Monday to Friday 8am to 5pm), these services are supported on a best effort basis. There is no implied commitment to a fault resolution or restoration time frame in the event of a service failure occurring outside normal working hours. Should such a level of support be required explicit negotiation will need to be undertaken with Information technology Services.

   Faults can be reported to the ITS Help Desk between 8.30am and 5pm Monday to Friday.

Document management control:

Prepared by: Chief Information Officer
Owned by: AVC, Finance, IT, Strategy, Commercial
Authorised by:
Date issued: 1 September 2004
Last review: September 2007
Next review: September 2009

---

[1] Information on how to effectively destroy data is available from Information Technology Services