IT USER REGULATIONS

1. Purpose and Scope

This document sets out the responsibilities and required behaviours of all users of University of Reading provided IT facilities and systems.

1.1 This policy applies to all:

- University of Reading staff.
- University of Reading students.
- Third party users authorised by the University of Reading or any department thereof.

1.2 This policy applies to all IT facilities and systems owned, leased, hired or otherwise provided by the University of Reading, connected directly or remotely to University infrastructure or used on University premises, including (but not limited to): fBd ( )T (t)uTd ( )T [u)3

packages.

- Data that the university provides, or arranges ac
  journals, datasets or citation databases.
- Online services arranged by the University, such as
- Access to the network provided or arranged by
  example, network connections in halls of residence
  to the internet from University PCs.

2. Roles and Responsibility

2.1 It is the responsibility of all users of the University of Reading's IT facilities and systems to:

- Read, understand and comply with this and other related policies.
- Ensure that their behaviour and activities when using University of Reading IT facilities is in accordance with the requirements of this policy.

2.2 The Director of DTS has day-to-day operational responsibility for the regulations and will review these regulations from a legal and operational perspective on an annual basis.

2.3 Managers have a responsibility to ensure the application of these regulations and members

4.6 You are responsible for the security of any computer terminal used by you. You should lock your terminal or log off when leaving it unattended and ensure it is switched off on leaving the office, to prevent unauthorised users accessing the system in your absence. Anyone who is not authorised to access the University network should only be allowed to use terminals under supervision.

4.7 Staff must ensure that they have up-to-date Anti-Virus software installed plus a firewall running at all times on equipment connected to the University of Reading network, including equipment not owned by or supplied by the University.

4.8 Any device that is not compliant with the above criteria is liable to physical or logical disconnection from the network without notice.

4.9 Serious damage or the theft of electronic communications equipment should be reported to the relevant campus security office which will advise the University Insurance Officer and the

websites of a dubious nature, downloading files from untrusted sources, opening email attachments/links in emails from people you do not know, or inserting media that have been created on compromised computers.

4.19 The University has taken measures to safeguard the security of its IT infrastructure, including things such as antivirus software, firewalls, spam filters and so on. You must not attempt to subvert or circumvent these measures in any way.

4.20 You should exercise particular caution when opening unsolicited e-mails from unknown sources or an e-mail which appears suspicious (for example, if it contains a link to a web.

Document control