



POLICY

ACCEPTABLE USE

iTEL takes the view that the following behaviours are unacceptable uses of the Internet:

1. **SPAM:** including sending or causing the sending of any unsolicited or unauthorized advertising, promotional materials, junk mail, bulk unsolicited email, mail bombing, chain letters, multiple newsgroup cross-posting, or other form or solicitation;
2. **BENEFITING FROM SPAM:** including hosting any website which, on a regular basis, is advertised by any person sending unsolicited commercial email or unsolicited bulk email or spam;
3. **EMPLOYING IDENTITY-DISGUIISING TECHNIQUES IN CONNECTION WITH SPAM:** including relaying email via a third party's mail server without permission, hosting an open mail relay server, or employing similar techniques to hide or obscure the source of an email;
4. **BREACHING INTELLECTUAL PROPERTY RIGHTS:** including hosting any content which infringes any copyright, trademark, trade secret, patent or other property or other intellectual property rights of any third party unless you are the owner of, or have the permission of the owner to post or transmit the content;
5. **SPREADING VIRUSES:** including knowingly hosting or transmitting any content that contains any software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment.
6. **HOSTING CONTENT WHICH IS UNLAWFUL/CRIMINAL:** including hosting or transmitting any content the hosting or transmitting of which would be a contravention of any law of the Commonwealth of, or a State in, Australia, such as, for example, material of a pornographic nature depicting children; and

7. MALICIOUS ACTIVITY AGAINST OTHER HOSTS ON THE INTERNET;
including:

- (i) defacing of web-sites without the permission of the website owner;
- (ii) obtaining (or attempting to obtain) un-authorized access to data by circumventing (or attempting to circumvent) security controls designed to prevent un-authorized access;
- (iii) the use of 'probing' devices on the internet with the intent of searching for and/or identifying security weaknesses on those devices;
- (iv) interference with service to any user, host or network including, without limitation, mailbombing, flooding, deliberate attempts to overload a system and broadcast attacks and denial of service attacks.

Date of Approval: 22 January 2003