APPENDIX B **Computer Safety**

Adapted from Sample Cyber-safety Use Agreement for Staff,
Internet Safety Group, April 2003
See *www.netsafe.org.nz* for further information

Computer Safety Use Agreement

A General Policy

Use of the Internet and other communication technologies by staff and guests is limited to usage appropriate to the ministry environment; including educational, informational, communication, staff professional development, and personal usage.

- Any incident involving material which is deemed 'objectionable' under the Films, Videos and Publications Classification Act 1993 could constitute criminal misconduct necessitating the involvement of the Police.
- Any involvement with any material which, while not illegal under the Act, is nonetheless detrimental to the integrity and safety of the ministry environment, may constitute professional misconduct serious enough to require disciplinary action.

B Staff use

All staff wishing to access the Internet on ministry equipment will be provided with tools necessary and appropriate for their position.

- All staff wishing to access the Internet on ministry equipment will be provided with an individual login user name and password. This needs to be kept confidential and not shared with anyone else; any illegal and/or inappropriate use of the computer facilities can be traced to the perpetrator by means of this login information.
- Staff will be provided with individual e-mail accounts.
- Links to appropriate websites can be placed on the ministry web pages to provide quick access to particular sites.
- Staff members need to be aware of confidentiality and privacy issues when accessing participant information via a network or the web.
- If a staff member ever wishes their own child to make use of the Internet equipment, the parent must be present at all times and is fully responsible for the conduct of their child, who would use the parent's login.
- If the Internet and other communication technologies (e.g. mobile phone) are used to facilitate misconduct such as harassment or involvement with inappropriate or illegal material, this could result in disciplinary action. Illegal material or activities will also necessitate the involvement of law enforcement.

C Ministry Website

This should be an on-going project. A number of important reasons exist for having a website, including providing information about the ministry and publishing articles and other work. See your Diocesan Office for further information.

D Monitoring

- Current Internet systems allow a record to be kept of which sites are visited, how often, and from which computer and log-in.
- Filtering software will be deployed where appropriate to restrict access to certain sites.
- If deemed necessary, auditing of the computer system could include all aspects of its use e.g. personal network storage folders and e-mail accounts.

E "Cyber-safety" Use Agreement for Staff

Please fill in and sign the following form regarding Safety, Professional Development, and your agreement to the Organisation's Policy.

This agreement should be copied and forwarded to your Board/Committee or Employer.

Guest Safety: (tick one)

❑ I have the appropriate knowledge to safely supervise Internet use.
❑ I need training in basic "Cyber-safety" issues before I supervise Internet use.

Staff Professional Development: (tick one)

❑ No professional development on Internet use is required at present.
❑ I would like additional training in Internet use.

I understand and agree to follow this Computer Safety Use Agreement as it applies to use of Internet and other communication technologies by staff, and by guests under the direction of staff.

Name:

Date:

Signature: