FALMOUTH UNIVERSITY

Falmouth Exeter Plus

Computer Users Agreement

Information Security Policy
2016

Falmouth Exeter Plus
Falmouth University
Information Security
Policy

Title :	**Computer Users Agreement**
Document Reference :	**ISP015**
Status :	**Draft**
Version :	**0.4**
Date :	**July 2016**
Classification :	**Public**

In order to be able to use the IT facilities and the campus network, you must firstly agree to the following rules and regulations.

Please read this information very carefully. Once you have agreed to these rules, you will then be issued with your password and email address.

Prior written agreement from your University must be sought for:

- Commercial use of campus network
- Loading software onto machines, other than that provided by the University via IT Services
- Accessing sites that may be deemed inappropriate

Falmouth University and the IT Services team seek to maintain a safe and healthy working environment to support its students in their activities. Users who receive abusive or threatening emails or who believe for whatever reason, that an IT facility is being used inappropriately, should consult the Director of IT Services, Falmouth Exeter Plus, or their Course Leader.

Any user to be found in breach of this computer user agreement will be barred from using the IT facilities (including the network) on the university campuses, and further action may be taken in accordance with the offence and statutory legal requirements.

Unacceptable Use

The campus network must not be used for any of the following:

- The creation, transmission or retrieval of any illegal, offensive, obscene or indecent images, data or other material; any data capable of being resolved into illegal, obscene or indecent images or material; or any web sites that give reference to them.

- The creation, transmission or retrieval of any terrorist or extremism-related literature, data or material in accordance with Government guidelines without obtaining specific, prior permission in writing (refer to the 'ISP010 - Accessing Sensitive Sites for Academic Purposes' procedure.

- The creation or transmission or retrieval of material which is designed or likely to cause annoyance, inconvenience or needless anxiety;

- The creation or transmission or retrieval of defamatory material;

- The transmission of material that is confidential to the University and/or the creation or transmission of material intended to undermine University policy.

- The transmission of material such that this infringes the copyright of another person;

- The transmission of unsolicited commercial or advertising material either to other User organisations or to organisations connected to other networks;

- Deliberate unauthorised access to facilities or services accessible via the campus network;

- Deliberate activities with any of the following characteristics:
    - Wasting staff effort or networked resources, including time on end systems accessible via Campus Network and the effort of staff involved in the support of those systems;
    - Corrupting or destroying other users' data;
    - Violating the privacy of other users;
    - Disrupting the work of other users service to other users (for example, deliberate or reckless overloading of access links or of switching equipment).
    - Other misuse of Campus Network or networked resources, such as the introduction of "viruses"

All information transmitted and retrieved via the internet is monitored and logged for security/safety purposes. Attempts to access certain sites (including sites which may contain extremism-related content) may trigger a warning to the user and are logged and reported for review. Information regarding individual user's use of the IT network and facilities, and information transmitted or retrieved via the internet may be used as part of safeguarding or disciplinary procedures and may also be provided to external authorities.

Any access to inappropriate sites (as classified by FortiGuard URL Database Categories, which are based upon the Web content viewing suitability of three major groups of customers: enterprises, schools, and home/families) will be highlighted to the user, and any onward access will be logged.

Reporting of access to these locations may be undertaken under the process documented within ISP018 – Investigation of Computer Use Policy. Information regarding individual's use of the IT network and facilities, and information transmitted or retrieved via the internet may be used as part of safeguarding or disciplinary procedures, and may also be provided to external authorities.

If access is required to sensitive material, then an application may be made by following the process documented in ISP010 – Access to Sensitive Material.

You are responsible for any use of the IT facilities and network conducted through your IT account. You must NEVER let other people use your username or reveal your password to anyone.