

FTEL Network Usage Policy

Ian G Batten

\$Id: policy.tex,v 1.1 2002/03/11 12:12:37 igb Exp \$

Contents

1	Introduction	1
1.1	Purpose of Document	1
1.2	Legal Implication	2
2	Usage Guidelines	2
2.1	System Ownership	2
2.2	Data Ownership	2
2.3	Prohibited Use	2
2.4	Personal Use	3
2.5	Security	4
2.6	Control	4
2.7	Export Control	4
2.8	Intellectual Property Rights	4
2.9	Confidentiality	5
2.10	Email Use	5
2.11	Usenet Use	5

1 Introduction

1.1 Purpose of Document

This document describes the expected standards of usage to be followed when using computers owned or operated by FTEL, the Fujitsu group, their customers, suppliers or partners. It also applies when data held on such computers is accessed

from other systems. For convenience, in the rest of this document “FTEL” should be understood to include these wider cases.

The purpose of this document is not to impose an arbitrary set of rules, but to protect the interests of both the users and the businesses and provide guidelines for safe and responsible usage.

1.2 Legal Implication

You may also have rights and responsibilities laid down in UK and European legislation, and nothing in this document should be taken to either remove your rights, or imply that sections of legislation do not apply to you. If you become aware of a conflict between this document and legislation, please notify the HR department.

2 Usage Guidelines

2.1 System Ownership

Computers are used within FTEL and its associated companies for business purposes. Computers and data are used in the course of business, and are not the property of the users. Some systems will be for practical purposes be used by one person: desktop systems and laptops, for example. These are not the property of the user, and should not be regarded as such. FTEL IS, HR and other staff have the right to access all systems, irrespective of type, unless limited by legislation.

2.2 Data Ownership

Data created by users on FTEL systems is the property of FTEL, not the user, and any exceptions to this should be negotiated with IS. If you believe you are holding data on FTEL systems which is protected under the Human Rights Act, you should discuss the matter with HR. FTEL IS, HR and other staff have the right to access all data, irrespective of type, unless limited by legislation.

2.3 Prohibited Use

Certain activities are prohibited under all circumstances, either in terms of access to types of data or patterns of use. Any user asked to breach these rules in the

course of business should immediately contact HR or IS: instruction of line manager does not override these directives, nor does a claimed business need. The main forbidden activities are:

- Access, storage or transmission of material that has an overt sexual content, whether illegal or otherwise. The test here is not illegality, but anything which would not be acceptable for open display in the workplace. It is unlikely that ambiguous cases will arise in the course of business, but any such case should be referred to HR.
- Access, storage or use of software outside the terms of licenses. This includes the use of software which is not correctly licensed or “shareware” software which has not been registered where required. The use of free software and open source software is permitted, but any use in a development context should be approved by technical management to ensure there is no impact on the intellectual property rights of FTEL. Users can assume that software installed and supported by IS is suitably licensed.
- Storage, development or any other dealing with viruses.
- Access, storage or use of material outside the terms of copyright. This covers most MP3 use unless the copyright terms explicitly permit it.
- Port scanning, password cracking and any other activity which might be reasonably construed as being an attempt to breach FTEL security, either from within or outside the FTEL network. IS are always happy to work with experienced security workers, and we will discuss security testing and, at our discretion, issue permission for people to run tests against our site. However, unauthorised activities will be assumed to be hostile.

2.4 Personal Use

Reasonable personal use, which does not conflict with the users’ job tasks or resources required by other users, is permitted subject to the permission of line management. The following activities are, however, explicitly forbidden:

- The circulation of mail containing jokes, pictures and other non-business material to lengthy address lists.

- Any use that may be construed as related to non-FTEL business activities of the user.
- Use of an FTEL email address for any purpose other than direct communication with individuals known to you, retail businesses with which you are trading or non-commercial organisations with which you have personal dealings.

A policy such as this is inevitably hard to draft, and we wish to allow users reasonable freedom of use without exposing the business to risk. If you are uncertain, please discuss the matter with HR.

2.5 Security

Users are expected to take reasonable measures to ensure the security and integrity of FTEL data, to prevent unauthorised access and modification. Security Guidance is available in another document.

2.6 Control

Users will follow policies and directives of FTEL's IS department, HR department or other appropriate bodies, as well as their line management.

2.7 Export Control

FTEL does not in the normal course of business hold data which is subject to export control, and business within the European Community does not require export control. However, you may need to transfer data which you are concerned requires further documentation, particularly anything involving cryptography. In this case, you should discuss the matter in detail with Commercial group.

2.8 Intellectual Property Rights

You should ensure that any intellectual property rights associated with material you transfer are correctly managed. If working with companies within the Fujitsu Group, or with whom we have an established contractual relationship, agreements should be in place. However, for the avoidance of doubt, you should discuss anything of which you are not certain with Commercial group.

2.9 Confidentiality

Explicitly or implicitly you have a duty of confidentiality to your employer. Any use you make of FTEL's computer systems must be consistent with this. If you are uncertain as to the precise nature of the confidentiality agreement you are subject to, you should ask HR to show you the details.

2.10 Email Use

Email has developed over the past ten years from a curiosity to the key means of communication for most business. When you use FTEL's email system, your mail is easily traceable to FTEL, and FTEL may be held liable.

The following activities are forbidden:

- Mail which may cause offence, be illegal under UK law or risk libel or slander actions.
- Mail which may be taken to bind FTEL to commercial or other agreements, unless you are explicitly empowered to do this.
- Circulation of chain mail, lists of jokes, pictures, virus warnings or other material not related to business.

2.11 Usenet Use

FTEL has a Usenet feed, and users have historically been permitted to post material to the net. You should ensure that:

- Your postings are acceptable under the email policy, above.
- You do not post material related to FTEL's business activities without discussion with commercial group.
- You do not cause FTEL's name to be associated with extreme opinions.

It is suggested that if you are posting to Usenet from FTEL computers, you obtain your own domain and cause your postings to be credited to that address.