STUDENT IT ACCEPTABLE USE POLICY

This document sets out the policy for students using the FX Plus supplied network facilities

ORGANISATION: FX PLUS

APPLIES TO: STUDENTS

POLICY OWNED BY: FX PLUS IT & DIGITAL (ON BEHALF OF FALMOUTH UNIVERSITY

REQUIRED CONSULTEES: NOT APPLICABLE

APPROVED BY: Joint Information Assurance Board

DATE APPROVED: TUESDAY, 07 SEPTEMBER 2021

REVIEW DATE: MONDAY, 09 SEPTEMBER 2024

STUDENT IT ACCEPTABLE USE POLICY

Falmouth Exeter Plus ("FX Plus") provides computing and networking facilities to support the delivery of services for Falmouth University located on Penryn and Falmouth Campuses. This document summarises the key responsibilities and required behaviour of all students of Falmouth University relating to the use of campus computers and information systems.

1 PURPOSE

1.1 This policy details the conditions that must be complied with when using University supplied computers and network facilities, whether located on campus or working remotely, or when using University supplied software via a third-party internet connection.

2 SCOPE

2.1 All Students of Falmouth University using IT facilities on the Penryn and Falmouth Campuses

3 KEY DEFINITIONS

3.1 'Service User' applies to any individual with access to the FX Plus network or computing resources.

3.2 The term 'computer' or 'computing resource' within this policy extends to devices such as tablets and smartphones as well as laptops/desktop computers, gaming devices, and the use of any software provided by the University for use by its students.

3.3 The term 'network communications equipment' within this policy refers to devices including, but not limited to: hubs, switches, routers, bridges, gateways, multiplexers, transceivers, hardware firewalls. and other control devices used to facilitate network usage within the University Network system.

4 KEY FACTS

You should familiarise yourself with the entirety of this policy and we would particularly draw your attention to the following clauses:

4.1 All network traffic is monitored for the prevention of criminal activity or activity which contravenes University policies. (Section 10 below)

4.2 All personal computing equipment should be kept up to date on security releases for your own protection. (Item 7.14 below)

4.3 There are several things that will not be considered acceptable to do on the University network. This includes things like crypto currency mining and torrenting. (Section 8 below)

4.4 You must protect yourself against computer misuse by others. All network activity is monitored against an item of equipment. If you allow others to use your login credentials, or don't lock your computer when you are not using it, allowing someone else to use your login, you will be accountable for their activity using your credentials. (Items 5.5 and 7.5 below)

4.5 If you see or are aware of a breach of this policy, you must report it to the IT & Digital Service Desk. Phone: 01326 213822, email: servicedesk@fxplus.ac.uk, Self Service: https://servicedesk.falmouth.ac.uk

5 GENERAL INFORMATION

5.1 Falmouth University must ensure that it complies with all relevant legislation, including (but not limited to) Regulation of Investigatory Powers Act (2000), Data Protection Act (2018), UK GDPR, Counter-Terrorism and Security Act 2015, Human Rights Act (1998), Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, Computer Misuse Act (1990) and the PREVENT Duty Guidance (2015).

5.2 Access to all University systems must be gained through a secure and IT approved authentication method, unique to, and identifiable of the individual.

5.3 Access to the internet is not guaranteed and may be affected by circumstances beyond the control of the University.

5.4 Passwords must have a minimum length of 10 characters and follow recognised complexity rules (a mix of upper-case and lower-case characters, including numerals).

5.5 You must ensure that you log out of University systems (including computers, applications, web pages etc) at the end of each session, particularly when using shared IT resources, such as suite computers.

5.6 All network communications and telephony equipment are managed by IT & Digital, or authorised contractors. It is forbidden to attempt to tamper with any such equipment.

5.7 It is strictly forbidden to attempt to connect any networking communications equipment which has not been authorised by IT & Digital to the campus network.

6 NETWORK USAGE

6.1 Only one computer/console may be connected to a network socket/port.

6.2 Computers must not operate as servers unless registered with, and authorised by, IT & Digital, except when specifically operating to provide shared gaming services.

6.3 Any user(s) generating excessive data network traffic will be asked to reduce that activity. Continued excessive usage will be in contravention of this policy.

6.4 Users will be held responsible for any breaches of this policy which have been committed by others by means of their connection or credentials.

7 NETWORK SERVICE USER RESPONSIBILITIES

All service users of the University computing facilities and network must:

7.1 Not knowingly perform any action that may be detrimental to the operation of the University network facilities.

7.2 Not knowingly operate any services which redistribute network services to others, nor otherwise provide access to services to those who are not entitled to access.

7.3 Report any breaches or suspected security incidents concerning the University network or computing facilities to the IT & Digital Service Desk immediately

7.4 Ensure computers are ‘screen locked’ when left unattended.

7.5 Never reveal or write down passwords, PINs, or any other unique authentication credential to anyone under any circumstance.

7.6 Change their password immediately if they believe it may have been compromised.

7.7 Not share a logged in session with anyone else. A Login ID identifies users as an individual and holds them directly accountable for all actions which take place under their credential.

7.8 Not use or attempt to use another individual's account.

7.9 Never knowingly use facilities in a manner which may introduce security or operational risk to the environment.

7.10 Never attempt to perform any unauthorised changes to university systems.

7.11 Immediately notify the IT & Digital Service Desk If they believe they have been granted access to IT systems, information or resources which are not appropriate or authorised to them.

7.12 Not facilitate, or attempt to facilitate, access for anyone else who is not authorised to access systems on the campus network.

7.13 Never copy, store, or transfer data or software owned by the University to any unmanaged device without written consent from the owner.

7.14 Ensure personal equipment is running supported versions of any installed operating systems or applications, with the most up to dates security patches installed, and an up-to-date and operational anti virus solution, where it exists for the product,

8 UNACCEPTABLE USE

Unacceptable use includes, but is not limited to, activities that:

8.1 Contravene English Law or Regulatory requirement, university policies or regulations.

8.2 Involve the creation, downloading, storage or transmission of unlawful material including material that is indecent, offensive, defamatory, threatening, discriminatory or extremist (as defined within the Prevent Guidance (2015)) in nature, or Data (in any form) that is capable of being resolved into such material. The University has a statutory duty to take steps to prevent individuals being drawn into extremism and terrorism, and a duty to alert and report any attempted access to, or dissemination of, such inappropriate material. If there is a genuine academic need to access material, the University must be made aware of this in advance and prior permission to access must be obtained from the Director of IT & Digital Services (Falmouth Exeter Plus) following the appropriate, formal, ethical approval being granted by the University.

8.3 May harm the reputation of Falmouth University, the University of Exeter, FX Plus or that of its staff and/or students.

8.4 Commit FX Plus or the University to any contractual obligations without obtaining the appropriate authority.

8.5 Involve the imitation or impersonation of another person, their network account, or their email address.

8.6 Attempts to undermine the security of the campus facilities, includes any unauthorised penetration testing or vulnerability scanning of any University systems.

8.7 Involve Cryptocurrency Mining, which is not permitted on the campus network.

8.8 Involve 'Peer-to-Peer' software (P2P). Such software is automatically detected and blocked. This applies to any P2P traffic, including legitimate transfers from sites using P2P transfer (torrents) for larger files, as the University has a duty to prevent the illegal downloading of copyright media, and the technical application of P2P prevents accurate assessment of the media being downloaded.

8.9 Provides access to facilities or information to unauthorised persons.

8.10 Involves creation and/or sending of unsolicited or unauthorised bulk email.

8.11 Involves creation, storing or transmitting any material which infringes copyright.

8.12 Involves any use of software which breaches its licensing agreement.

8.13 Attempts to deliberately gain unauthorised access to services on other networks.

8.14 Corrupts or destroys other users' data.

8.15 Violates the privacy of other users.

8.16 Disrupts the access for other users using the network (for example, deliberate or reckless overloading of access links or of switching equipment).

8.17 Facilitates the introduction of viruses or malware etc to the campus network.

9 BREACHES AND NON-COMPLIANCE

9.1 Any breach of this policy may result in the permanent or temporary withdrawal or restriction of access to network services.

9.2 Any breach of this policy may lead to disciplinary action being taken in line with the university's disciplinary procedure, which can be found at:
https://www.falmouth.ac.uk/student-regulations

9.3 If there is an actual or likely breach of information security, that access will be withdrawn until adequate controls are in place.

9.4 If you see or are aware of a breach of this policy, you must report it to the IT & Digital Service Desk. Phone: 01326 213822, email: servicedesk@fxplus.ac.uk, Self Service: https://servicedesk.falmouth.ac.uk

9.5 Failure to report any breach, or suspected breach of information security to IT & Digital service desk is deemed to be a breach of policy.

10 MONITORING

10.1 All network activity is monitored regardless of device used to connect to the network.

10.2 Authorised staff may access files and communications, including electronic mail files, stored on any IT facilities owned, managed, or provided by FX Plus or the universities and may examine the content of these files and any relevant traffic data.

10.3 FX Plus may access files and communications for the following reasons:

10.3.1 To ensure the operational effectiveness of its services (for example, the organisation may take measures to protect its systems from viruses and other threats).

10.3.2 To establish the existence of facts relevant to the business of FX Plus or the Universities (for example, where a case of suspected plagiarism is being investigated and there is sufficient evidence, the contents of an individual's communications and/or files may be examined without their consent with the authority of an authorised person).

10.3.3 To investigate or detect unauthorised use of its systems.

10.3.4 To ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the business of FX Plus or the Universities.

10.3.5 To comply with information requests made under the Data Protection Act or Freedom of Information Act.

10.4 The University may be legally obligated to carry out enhanced monitoring on behalf of UK law enforcement agencies.

10.5 Where the University is compelled to provide access to communications by virtue of a Court Order or other competent authority, the organisation will disclose information to these non-institutional bodies/persons when required as allowed under the UK Law.

11 EQUALITY IMPACT ASSESSMENT

The impact assessment process is currently being reviewed. This section will be updated following conclusion of the review.

12 CONTACT FOR FURTHER INFORMATION

FX Plus Information Governance – dataprotection@fxplus.ac.uk