STAFF IT ACCEPTABLE USE POLICY

This document sets out the policy for staff using network, computing and digital facilities supplied by their organisation.

ORGANISATION: FX PLUS, FALMOUTH UNIVERSITY, THE STUDENT'S UNION

APPLIES TO: STAFF

POLICY OWNED BY: FX PLUS IT & DIGITAL

REQUIRED CONSULTEES: NOT APPLICABLE

APPROVED BY: DIGITAL & IT GROUP (Falmouth University), SENIOR EXECUTIVE TEAM (FX Plus), THE STUDENTS UNION

DATE APPROVED: 27/07/22

REVIEW DATE: THURSDAY, 31 JULY 2025

Version Control			
Date	**Who**	**Details**	**Version No**
27/07/22	Dean Archer	Approved	1.0
14/11/22	Dean Archer	Re-worded Section 7.13	1.1

STAFF IT ACCEPTABLE USE POLICY

Falmouth Exeter Plus (“FX Plus”) provides computing and networking facilities to support the delivery of services for Falmouth University, the University of Exeter, The Students’ Union, FX Plus and its subsidiary commercial services, including, but not limited to Cornwall Plus, the Sports Centre and the Nursery, located on Penryn, Falmouth and Truro Campuses. This document summarises the key responsibilities and required behaviour of all staff relating to the use of campus computers and information systems.

1 PURPOSE

1.1 This policy details the conditions that must be complied with by all staff and contractors when using computing and/or network resources supplied by either Falmouth University, FX Plus (and its subsidiaries), or The Students Union.

2 SCOPE

2.1 The scope of the policy extends to all staff and contractors working for, or on behalf of, either Falmouth University, FX Plus (and its subsidiaries), or The Students Union. The requirements defined in this policy are applicable when using computing and/or network resources provided by the organisation, whether being used when located on campus or when working remotely.

3 KEY DEFINITIONS

3.1 ‘Service User’ applies to any individual with access to the organisational network or computing resources.

3.2 The term ‘managed device’ 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 organisation.

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 institutional network.

3.4 The term ‘organisation’ within the context of this policy refers interchangeably to Falmouth University, FX Plus (and its subsidiaries), and The Students Union.

3.5 The term ‘organisational network’ refers to any computing or network resource operating on the campus IT network, or connected to the campus IT network via a VPN connection.

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 organisational network traffic is monitored for the prevention of criminal activity or activity which contravenes your organisation’s 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 activities that are considered unacceptable to carry out on the organisational network. This includes crypto currency mining and torrenting. (Section 8 below)

4.4 All organisational 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 Organisations must ensure that they comply with all relevant legislation, including (but not limited to) Investigatory Powers Act (2016), 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 You must ensure that you log out of managed systems (including computers, applications, web pages etc) at the end of each session, particularly when using shared IT resources, such as suite computers.

5.3 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.

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

6 NETWORK USAGE

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

6.2 Devices must not operate as servers unless registered with, and authorised by, IT & Digital.

6.3 Any user(s) generating excessive network data traffic, which results in a degradation of performance for other users, 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 SERVICE USER RESPONSIBILITIES

All service users of the organisational network must:

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

7.2 Not knowingly operate any services which redistribute organisational 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 organisational 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 organisational 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 organisational network.

7.13 Never copy, store, or transfer personal data, proprietary information, or software owned by your organisation to an unmanaged device without written consent from the software license holder or data 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, the organisation’s 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 organisation 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 organisation 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)

8.3 May harm the reputation of the Organisation or that of its staff and/or students.

8.4 Commit the organisation 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 the organisation’s systems.

8.7 Involve Cryptocurrency Mining, which is not permitted on the organisational 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 organisation 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 organisational network (for example, deliberate overloading of access links or of switching equipment).

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

8.18 Involve uninstalling and/or reconfiguring anti-malware, updates, logging or other protective services on managed devices.

8.19 Involve sharing log-in credentials with another user.

8.20 Involve using personal email accounts to conduct the organisation's business.

8.21 Involve automatically forwarding emails from a staff email account to a personal account.

8.22 Involve personal benefit through discounts offered to students through the use of academic email addresses, where such discount is not available to staff.

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 organisational network services.

9.2 Any breach of this policy may lead to disciplinary action being taken in line with the HR Disciplinary Procedure for your organisation.

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 organisational network.

10.2 Authorised staff may access files and communications, including electronic mail files, stored on any IT facilities owned, managed, or provided by the organisations 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 the organisation (for example, where a case of suspected staff misconduct 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 ensure compliance with official regulations or organisational policies/procedures.

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

10.3.6 Where compelled to provide access to communications by virtue of a Court Order or other competent authority, the organisation will disclose information to those 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