Far Western University

Information Technology Guidelines

2023

Contents

Introduction

1.1 Background

As technology continues to play an increasingly important role in personal and academic lives, it is essential to ensure the secure and responsible use of IT resources at Far Western University. In order to develop and strengthen the university digitalization and automation, this Information Technology Guidelines, aligning with the University IT policy and strategy, has been prepared. The guidelines ensure the effective and responsible use of IT resources to protect sensitive information, mitigate risks, and align IT activities with university's vision and mission. All users of university IT resources need to be familiar with IT guidelines, and to take necessary steps to ensure that they are in compliance with its provisions.

1.2 Current Guideline Status

FWU has been taking some steps towards digitalization. Currently, it has some of the systems and practices in place including the following: Centralized email system (FWU domain); centralized website management system; account management system; exam management system; online results system. It also initiated online classes and exams during the COVID-19 pandemic. Meanwhile, it developed a policy guidelines titled "वैकल्पिक माध्यमबाट परीक्षा सञ्चालन, व्यवस्थापन तथा मूल्यांकन सम्बन्धी निर्देशिका, २०७७ (संशोधन सहित २०७८)". Likewise, web-conferencing and remote guest sessions are also taking place. Importantly, university MIS is in place. FWU has a good internet connectivity to support the academic and administrative activities of the university. This way, FWU has done some work on IT and taken some basic steps in practice. However, prior to this, a consolidated IT guideline was non-existent.

1.3 Objectives

This guideline provides a framework for the effective and secure use of ICT resources within the university and beyond. It encourages good practice in the use of IT resources. Furthermore, it upholds the ideals of IT use as envisioned in the IT policy and strategies 2023.

1.4 The IT Users and Resources

The IT users include all those who use IT resources provided by the University, including but not limited to students, staff (teaching and non-teaching), casual staff, consultants, contractors and suppliers working for or on behalf of the university, visitors to the university. Likewise, the IT resources refers to all those ICT related resources and systems made available to the users by or on behalf of the university. Such IT resources include, but to be limited to the following:

- Personal computers and laptops
- Printers, copiers, scanners and multimedia devices

- Mobile devices such as smart phones and tablets
- Networks with wired, wireless, dialup and/or internet connections
- Internet and intranet services
- E-mail and other messaging, social networking or collaboration services
- System and application software, services and (research) databases, including learning management system, Moodle Learning Analytics, SPSS, JSTOR, IEEE Xplore, ScienceDirect
- Virtual meeting and document management tools/platforms with university subscription such as Zoom, Microsoft Teams, WebEx, Microsoft SharePoint, Google Drive, Dropbox, etc.
- VR and AR tools such as VR headsets, AR apps, and simulators
- Removable media such as USB drives

Key Digitalization Guidelines

2.1 Connectivity Guidelines

- Any user can approach the IT department to get access to reliable and uninterrupted network connectivity.
- Wired and wireless network connections will be properly configured and secured to prevent unauthorized access.
- Internet connectivity will be available across all locations with the university.

2.2 Digital Infrastructure Guidelines

- Authorized software and hardware configurations should be used to ensure compatibility, security, and supportability.
- Unlicensed or unauthorized software will gradually be strictly prohibited from being installed or used on university systems.

2.3 Virtual Learning Environment Guidelines

- Students, faculty, and staff should use their university-issued credentials to access the digital Learning Platform or LMS/VLE.
- User access privileges will be granted based on roles and responsibilities (e.g. manager, teacher, and student).
- Course materials, including syllabi, lecture notes, assignments, and assessments, need to be uploaded and organized in a structured manner.
- Clear instructions and guidelines for students need to be provided on how to navigate and utilize the VLE for coursework.
- Copyrighted materials should be used in compliance with intellectual property laws and university policies.
- Faculty and students should utilize VLE communication tools, such as discussion forums, messaging, and announcements, for course-related communication.
- Virtual meeting tools, such as video conferencing or chat applications, will be integrated within the VLE for synchronous communication and collaboration.
- The VLE supports various assessment methods, including quizzes, assignments, discussions, and online exams.
- Training and workshops will be provided to faculty and students to ensure effective usage of the VLE's features and tools.
- The university will conduct periodic reviews and evaluations of the VLE's performance, usability, and effectiveness.

2.4 EMIS Operation Guidelines

- Access to the EMIS should be granted based on user roles and responsibilities, following authentication protocols.
- Regular backups of EMIS data will be performed to ensure data availability and disaster recovery.
- Adequate user support will be available to address EMIS-related queries and issues.
- Regular monitoring of the EMIS infrastructure and performance should be conducted to ensure optimal system availability and response times.
- As per our IT policy, the EMIS will be integrated with other relevant university systems (as per UGC regulation) to ensure seamless data flow and interoperability.

2.5 Digital Resource Development and Dissemination Guidelines

FWU is committed to creating and sharing high-quality digital resources (E-library, digital studio and production, and publication of e-books, audio/video, animation, simulation, and gaming learning materials) that support innovation, foster knowledge sharing, and enhance learning while upholding intellectual property rights and data privacy regulations.

2.6 Human Resource Development Guidelines

The HRD section acts as one of the major policy implementers. It works on building capacity of its human resources on ICT competencies in collaboration with the ICT steering committee and the IT Director. It also strengthens the capacity of the system and equipment to smoothly run the ICT related activities. It also enables a system to protect university from IT related risks (e.g. cyberattacks). FWU takes the following strategies to make use of ICT for HRD:

a. **E-learning and training**: FWU prioritizes the use of ICT to offer e-learning and training programs to its employees. This can include online courses, webinars, and other forms of virtual training that can be accessed remotely.

b. **Virtual collaboration**: FWU prioritizes the use ICT tools such as video conferencing, collaboration software, and social media to facilitate virtual collaboration between employees. This can help to promote knowledge sharing, teamwork, and communication among staff members.

c. **Performance management**: FWU will use ICT tools to automate and streamline its performance management processes.

d. **Talent management**: FWU uses ICT tools to manage its talent pipeline more effectively. This can include using software to manage job postings, applicant tracking, and candidate screening. ICT can also be used to facilitate onboarding and training for new hires.

e. **Data analysis**: FWU will gradually use ICT tools to collect, analyze, and interpret HRD data. This can include using analytics software to track employee performance, identify skills gaps, and monitor training effectiveness.

4

2.7 University and Its Campus Office Automation Guidelines

- FWU is committed to implementing comprehensive university and its campus office automation solutions, including robust Education Management Information Systems (EMIS), to streamline administrative processes, enhance operational efficiency, and improve data-driven decision-making across all campus departments and functions.
- University e-governance will eventually be ensured (i.e., using an ERP system integrating finance and administration). .

2.8 IT System Security Privacy and Surveillance Guidelines

- Approved software and hardware configurations should be used to ensure compatibility, security, and supportability.
- Regular software updates, patches, and vulnerability assessments will be conducted to mitigate security risks.

2.9 Data Protection, Back up and Disaster Recovery Guidelines

- All data transmitted or stored within the university's digital infrastructure should be protected in accordance with applicable data protection laws and university policies.
- Adequate measures, such as encryption and access controls, will be implemented to safeguard sensitive data.
- Individual users should perform regular backups of their vital data. Users should keep their valuable data backups in external storage devices.
- Regular data backups should be performed to ensure data integrity and availability.
- A disaster recovery plan will be developed to ensure the rapid restoration of IT services in the event of a major disruption.

2.10 Online Exam Guidelines

- FWU will follow the existing "वैकल्पिक माध्यमबाट परीक्षा सञ्चालन, व्यवस्थापन तथा मूल्यांकन सम्बन्धी निर्देशिका, २०७७ (संशोधन सहित २०७८)".

2.11 Data Center or Cloud Operation Guidelines

- IT service requests and support need to be made through a centralized helpdesk system (IT Department).
- Adequate security measures should be implemented when storing or processing university data in the cloud.
- The university will increasingly use cloud-based collaboration tools such as Google Docs, Microsoft Teams, or Slack to enable more effective collaboration between personnel. This can include real-time document editing, chat functions, and project management tools.
- The university will provide training and support to personnel to ensure that they are able to use cloud-based technology effectively and securely. This can include online training

modules, one-on-one coaching, and regular updates on new features and security best practices.

- Cloud service providers will be evaluated for their security, privacy, and compliance standards before engaging their services.

2.12 Plagiarism Detection Guidelines

- FWU will use a paid plagiarism detection software.
- For student research purpose, 15% plagiarism level will be accepted.
- For faculty research, the acceptable plagiarism level is below 10%.

2.13 Website and Email Operation Guidelines

- E-mail service authorized by FWU (with university domain) shall only be used for all official correspondence.
- Users of the University's systems must not send abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory emails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a student or member of staff via email, should inform their HOD/Principal/Campus Chief.
- The University reserves the right to suspend a user's email account as a result of any suspected misuse or breach of this guideline.

2.14 University Centralized E-attendance guidelines

- The purpose of the centralized e-attendance system is to accurately record and monitor attendance for students, faculty, and staff across the university.
- Faculty and staff members should record their attendance through the e-attendance system.
- The e-attendance system will integrate with the university's course management system to streamline attendance tracking for each course or module.
- Students are required to mark their attendance through the designated e-attendance system for each class or session.

2.15 Limited Personal Use

Users will use ICT resources for authorized purposes, such as official university activities or university approved research and development, and limited personal use. The university allows limited personal use of the internet and electronic communications facilities. Personal use may be monitored. Users will consider the following conditions for personal use:

a. The university is not impacted financially.
b. University business objectives are not unduly impacted.
c. Personal use does not breach any university rules.

Roles and Responsibilities

ICT Steering Committee

- Act as an apex body for IT resource related matters.
- Propose and develop other guidelines/policies as and when required
- Form any working groups or task force as and when needed
- Approve and authenticate IT related policy, strategy and guidelines
- Follow the responsibilities of the users

IT Subcommittees

- Serve as task force for relevant IT component, in recommendation of the ICT Steering Committee
- Report to the ICT Steering Committee
- Follow the responsibilities of the users

IT Department/Unit and IT Director

- Serve as a focal point for IT policy implementation
- Hold an authorized staff member status. Such status will be displayed on their university identification.
- Establishing adequate controls to comply with this procedure.
- Establishing an ongoing information security awareness campaign intended to raise user security awareness when using the university's ICT Assets.
- Oversee and provide authority to authorized staff members to monitor and audit the use of ICT assets
- Handle and troubleshoot security incidents and any identified weaknesses.

Responsibilities of the users

(Any member of the University Community who uses or accesses an ICT asset)

- Users are expected to use university IT resources in a responsible and ethical manner, and to comply with all applicable laws and regulations. This includes refraining from activities such as hacking, spamming, and illegal file sharing.
- Users are required to take appropriate measures to protect their devices and accounts from unauthorized access, such as using strong passwords, enabling two-factor authentication, and keeping software up-to-date.
- Users are responsible for safeguarding any confidential or sensitive information that they access or store using university IT resources. This includes complying with data protection laws and regulations, and reporting any data breaches or security incidents promptly.
- Users are required to report any suspected violations of this policy or any other IT-related issues to the appropriate authorities, such as the IT staff or the IT Director.

Compliance and Reporting

- All users should comply with this guideline.
- They should report security incidents and any identified weaknesses to the IT Director/ IT staff immediately.

Review and Revision

- Future changes in this guideline, as and when deemed necessary, shall be made by the IT Department with the approval of the ICT Steering Committee.
- This guideline will be reviewed in every two years and revised in every four years.

Approval and Implementation

- This guideline has been approved on the following date and is put into effect on the same date.

Version	Approved/ Amended	Date	Committee/Board	Approval Decision/Minute Number	Key Changes
New	Approved	June 15, 2023	ICT Steering Committee	473	N/A

सुदूरपश्चिम विश्वविद्यालय
Far Western University

Information Technology Policy, Strategy and Guidelines 2023

Far Western University
+977-099-520729
info@fwu.edu.np
Bheemdatta Municipality-18, Mahendranagar, Kanchanpur