FRONTIER MEDICAL AND DENTAL COLLEGE

Policy on legal, Ethical and Safety measures related to Technology use for Students and Faculty

1. Purpose

The purpose of this policy is to establish clear ethical, legal, and safety standards governing the use of information and communication technologies by students, faculty, and staff of Frontier Medical and Dental College and Shahina Jamil Teaching Hospital. It aims to ensure that all digital and electronic resources are used responsibly, professionally, and in a manner consistent with institutional values, data protection laws, and medical ethics.

2. Scope

This policy applies to all students, faculty members, administrative personnel, and visiting professionals who access or use institutional technology resources, including but not limited to:

- Computers, servers, and networks owned or operated by the college or hospital.
- Institutional email systems, online learning platforms, and official social media channels.
- Electronic health records and patient data systems.
- Digital teaching aids, audiovisual material, and online communication tools.

3. Policy Statement

(a) The institution recognizes that technology is integral to medical education, patient care, and research, but its use must remain within the bounds of professionalism, confidentiality, and ethical conduct.

(b) All users are expected to exercise honesty, integrity, and responsibility in their digital activities.

(c) Any misuse of technology that compromises privacy, breaches patient confidentiality, violates intellectual property rights, or brings disrepute to the institution shall be treated as a serious offence.

4. Legal and Ethical Compliance

(i) Users shall comply with applicable Pakistani laws relating to cybercrime, copyright, data protection, and digital communication, including the *Prevention of Electronic Crimes Act, 2016 (PECA)*.

(ii) Faculty and students shall respect patient privacy in accordance with the institutional "Privacy and Confidentiality of Patient Policy" and PMDC Code of Ethics.

(iii) All use of technology must reflect academic integrity — plagiarism, unauthorized data access, and falsification of records are strictly prohibited.

(iv) Users must not download or transmit illegal, defamatory, or discriminatory content.

5. Safety and Data Security

(a) Access to institutional systems shall be protected by individual user credentials; sharing passwords is prohibited.

(b) All patient and institutional data stored electronically must be encrypted and accessible only to authorized personnel.

(c) Personal devices used for official purposes (e.g., mobile phones, laptops) must follow the same security standards as institutional devices.

(d) No unauthorized software, external storage, or cloud service shall be used to store or transfer institutional information.

(e) The IT Department shall conduct periodic audits, and vulnerability checks to ensure compliance.

6. Professional Conduct in Digital Spaces

(i) Faculty and students shall maintain professionalism in emails, messages, online classes, and public posts.

(ii) Official communication must occur only through authorized institutional channels.

(iii) The use of social media must uphold the dignity of the medical profession and the reputation of the institution; posting patient images, information, or hospital content without written authorization is strictly prohibited.

(iv) Cyberbullying, harassment, or any form of online misconduct shall result in disciplinary action under institutional rules.

7. Monitoring and Enforcement

(a) The disciplinary committee will be responsible for monitoring implementation and addressing reported violations.

(b) The Committee may investigate complaints, recommend corrective actions, and impose sanctions where necessary.

(c) Users may appeal against any disciplinary decision before the principal, whose decision shall be final.

8. Education and Awareness

(i) All incoming students and faculty members shall receive orientation on digital ethics, cybersecurity, and data protection.

(ii) Annual workshops would be organized to reinforce safe technological practices and inform users of updated legal obligations.

9. Violations and Penalties

(a) Violations of this policy, including unauthorized access, data breach, cyber misconduct, or misuse of institutional systems, shall constitute gross misconduct.

(b) Offenders shall face disciplinary proceedings, suspension of digital privileges, termination (in case of staff), or referral to law enforcement where applicable.

10. Review and Amendment

This policy shall be reviewed biennially or earlier if required by changes in legislation, institutional practice, or technological developments. The updated version shall be circulated to all departments and uploaded to the official institutional portal.