Greystone Institute Online Usage Policy

The purpose of this Online Usage Policy is to ensure that all students, faculty, and staff at Greystone Institute use the internet and computer facilities responsibly, ethically, and securely. This policy aims to mitigate risks associated with internet usage and outline appropriate and restricted uses of the Institute's technological resources.

Definitions

Internet Usage: Accessing the internet via any device connected to Greystone Institute's network.
Computer Facilities: All hardware, software, network resources, and communication systems provided by Greystone Institute.
Malicious Activities: Activities intended to harm or exploit systems, networks, or individuals.

Recognizing Risks of Internet Usage

Security Threats: Including malware, viruses, phishing, and hacking attempts.
Data Privacy: Risks of unauthorized access to sensitive or personal information.
Reputational Damage: Potential harm to the Institute's reputation through inappropriate or illegal online activities.
Legal Compliance: Risks associated with non-compliance with laws and regulations.

Appropriate Use of the Internet and Computer Facilities

Educational and Professional Use: Internet and computer facilities should primarily be used for educational purposes, research, academic activities, and professional development.
Communication: Using Institute-provided email and communication tools for academic and administrative communication.
Collaboration: Utilizing online tools and platforms for collaboration on academic and administrative projects.
Research: Accessing online libraries, databases, and other resources for research and study purposes.
Personal Use: Limited personal use is permitted, provided it does not interfere with work, study responsibilities, or violate any part of this policy.

Restricted Uses

Illegal Activities: Engaging in activities that violate local, state, federal, or international laws, including copyright infringement and unauthorized downloading or sharing of files.
Malicious Activities: Creating, transmitting, or distributing harmful software or engaging in activities intended to disrupt or compromise systems or networks.
Inappropriate Content: Accessing, downloading, or sharing obscene, offensive, or inappropriate material, including pornography, hate speech, or material that discriminates based on race, gender, religion, or other protected characteristics.

Unauthorized Access: Attempting to access or use accounts, data, or systems without proper authorization.
Commercial Use: Using Institute resources for commercial purposes, personal gain, or outside business activities without authorization.
Excessive Personal Use: Engaging in personal internet usage that detracts from academic or professional responsibilities.

Security Measures
Passwords: Use strong, unique passwords and keep them confidential. Change passwords regularly and immediately report any suspected compromise.
Software Updates: Ensure that all software, including antivirus programs, is regularly updated.
Network Access: Access the Institute's network only through authorized devices and secure connections.
Data Protection: Protect sensitive data by using encryption, secure storage solutions, and adhering to data privacy regulations.

Monitoring and Enforcement
Monitoring: The Institute reserves the right to monitor internet and computer facility usage to ensure compliance with this policy.
Reporting Violations: Any violations of this policy should be reported to the IT Department or relevant authority immediately.
Disciplinary Actions: Violations of this policy may result in disciplinary actions, including loss of access privileges, academic or employment suspension, termination, or legal action.