Acceptable Use of IT Resources

1. Purpose

The purpose of this policy is to set and communicate the terms and conditions for acceptable use of IT resources at Qatar University.

2. Definitions

Term	Definition
Computing Device	A laptop, desktop, mobile or other device used at Qatar University to access institutional data, systems, and network.
QU-Owned Device	A computing device that is owned by Qatar University, regardless of the custodian.
QU-Managed Device	A device that is managed by the IT Services Department, regardless of ownership.
QU-Supported Device	A device that is supported by the IT Services Department, regardless of ownership.
QU IT Resources	All IT resources provided by Qatar University for its constituents, including computing devices, services, digital resources, infrastructures resources such as network and Internet access.

3. Scope

This policy applies to all users of any QU IT resources.

4. Acceptable Use Terms

Qatar University provides its users with information technology resources to support the academic, educational, administrative, public service, and research activities.

Users are responsible for adhering to the highest standards of ethical, considerate and proper use of such resources to serve these purposes, regardless of their affiliation with the University.

All users of QU IT resources are required to adhere to the policy sections below.

4.1 General Terms

Acceptable Use

The use of QU IT Resources should be for the purposes that are consistent with the non-profit educational mission and policies and legal requirements of the University, including license agreements and terms of service of the University.

Users may use only the QU IT Resources for which they have authorization and for the purpose of conducting QU business.

Prohibited Use

The use of QU IT Resources should not violate local applicable laws or applicable university policies. Regardless of the source of use or location of the user, QU IT Resources may not be used to transmit malicious, harassing or defamatory content.

Users are prohibited from use other users' accounts or attempt to capture or guess other users' passwords or credentials.

Users are also prohibited from providing unauthorized users access to QU IT Resources.

Accountability

Users of QU IT Resources are individually responsible and accountable for the appropriate use of the resources assigned to them or which they are authorized to access.

4.2 Use of Computing Devices

Users of QU-owned and QU-managed devices acknowledge and accept the following:

1. QU-owned devices are the property of the University. Users should handle them responsibly and with care to avoid breaking, failure and physical damage.
2. The IT Services Department (ITS) maintains control over the configuration of their device(s) and is the final authority on what can be installed on these devices.
3. Users should not expect to have administrative privileges on QU-owned or QU-managed devices.
4. Users should not attempt to format or repair a University-managed computing device;

Users shall not use their computing devices to:

1. access illegally or without authorization: data, computers, accounts, or networks;
2. distribute offensive, abusive and/or harmful material;
3. knowingly install or distribute computer malware or other malicious software that could potentially harm systems, cause loss of data, or disrupt network services;
4. attempt to circumvent any established security measures to gain access to confidential and restricted information;
5. install or copy unlicensed software;
6. create, transmit or participate in pranks, hacking schemes, chain letters, false or deceptive information, or any other fraudulent or unlawful purposes;
7. violate local or international laws and regulations or other contractual obligations.
8. Attempt to format or repair a University-owned computing device

4.3 Use of Imaging Devices (Printers, Scanners, Copiers)

1. Printing, scanning, and copying devices and materials provided by QU are the sole property of QU and should be used for University business only.
2. Users should consider the surroundings when printing or copying confidential information, and should promptly remove the printed material from the printer.
3. Users shall not:
    a. attempt to move or remove printers and scanners from their locations without prior consent of ITS;
    b. attempt to fix a printer or scanner without contacting the ITS Service Desk for support;
    c. print or distribute abusive, offensive or unethical material.

4.4 Use of Electronic Mail

Users of QU-provided email accounts acknowledge and accept the following terms:

1. The use of electronic mail is a privilege extended by QU to its students, faculty, staff and others in order to facilitate communication in the course of conducting University business.
2. The University owns the content of electronic mailboxes of its faculty and staff and all others mailboxes created to facilitate University business, e.g. consultants and contractors.
3. The Information Technology Services Department (ITS) is responsible for managing and supporting the University's email services.
4. ITS may provide access to, or copies of the content of, mailboxes as required by QU business and/or in the course of a security forensic investigation.
5. Email accounts may be disabled:
    a. when an employee's association with the University ends. Exceptions may be granted for a specified period of time if such access is required to fulfill a business need.
    b. if they are linked to security incidents such as SPAM or other inappropriate use of email.
6. **QU employees:**
    a. Shall restrict the use of their QU mailbox to QU-related communication.
    b. Shall not use their QU email address for any personal activities such as registering on online sites.
    c. Shall not forward their QU mail to non-QU systems such as cloud-based email services.
    d. Shall not make offline copies of their mailboxes which may expose them to unauthorized disclosure.
    e. Do not have the right to take copies of their email when their association with the University ends.
7. **All Email Users:**
    a. Shall not share passwords, credit card information, and other restricted data through email without proper protection such as encryption.
    b. Shall not transmit offensive, abusive, violent, threatening and harmful content through email.
    c. Shall not transmit, forward, or post internal emails or attach classified documents containing confidential information to anyone outside of QU.

   d. Shall not transmit, forward, or post chain letter emails to anyone at any time.
   e. Shall not falsify or impersonate a sender address.
   f. Shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of QU or any unit of the QU, while communicating with domains outside QU.
   g. Shall take proper precautions to avoid falling victims for phishing.
   h. Shall not circumvent existing controls for email access.
   i. Shall report any observed irregularities to ITS for further investigation.
   j. May not use mail broadcasting for personal, commercial, and non University-related communication.
   k. Should avoid sending mass emails to users unless content is relevant to all the recipients of the mailing list.

8. Bulk emails and mailing lists:
   a. Mailing lists are provided at Qatar University to facilitate sending emails to a large audience. However users should exercise caution whenever they are sending out bulk emails.
   b. Use of bulk email and mailing lists is for University related topics only. Users may not use mail broadcasting for personal, commercial, and non-University related announcements.
   c. Communications sent through mailing lists should be targeted to the related audience. Users should avoid sending mass emails to users unless content is relevant to all the recipients of the mailing list
   d. Users should consider the content of emails before broadcasting to mailing groups. Users are not allowed to abuse mailing lists by sending unsolicited emails or spam that may contain offensive, threatening or harmful material. In addition, users should not use mailing lists to send advertisements such as advertising a property for sale, car, personal achievement, etc., except through the use of the dedicated mailing list (or group if using the University portal).

4.5 Use of Network and Internet Access

Users accessing the Internet through QU are expected to use their access responsibly and ethically.

1. Users shall not compromise the University resources by knowingly downloading malicious, offensive, abusive, profane, illegal and/or harmful content.
2. Users should refrain from using peer-to-peer file sharing protocols due to the inherent risks associated with such use. Exceptions can be granted following proper assessment and authorization by the Information Security Manager.
3. Users shall not install or configure any active or passive network component without the express consent of ITS. This includes, but is not limited to:
   a. Network access equipment (wired or wireless)
   b. Network servers (e.g. DHCP, DNS, etc.)
   c. Any device that consumes a disproportionate amount of network bandwidth.
   d. Any device that can bypass the security mechanisms enforced by the University.

4. Users shall not bypass the security mechanism implemented and managed by QU for accessing the Internet.
5. Users shall not install devices or software that allow them direct access to their devices or systems without going through the existing security controls such as firewalls or VPN devices. Methods such as modems attached to devices or remote access software such as PCAnywhere can pose a great risk to the QU infrastructure and inadvertently allow perpetrators direct access to internal QU resources.
6. Users are solely responsible for any indirect, consequential, special or punitive damages or losses that may arise from their inappropriate use of the Internet access.
7. Users may submit requests to adjust content filtering or Internet access restrictions from the ITS Service Desk. ITS will assess the risks associated with implementing the request and retains the right to reject any requests that may present a security risk to the University's internal network and/or IT resources.

4.6 Telecommunication Services (Telephones)

QU uses IP phones (hardware and software) to provide telephone services to its employees. Users:

1. Should handle the phones with care and report any hardware or configuration issues to the ITS Service Desk.
2. Should protect their phone PIN, especially if they have access to make long distance calls.
3. Must not abuse their long distance access privileges. Reported abuses may result in disciplinary action.
4. Use emergency phones that are distributed around campus for emergency purposes only.
5. Must return the IP phone hardware to the ITS Service Desk during the exit clearance process.

4.7 Use of Social Media

QU users of social media sites shall NOT:

1. Share QU information through social media platforms.
2. Use their personal accounts to communicate work-related information.
3. Post pictures or information that link them to QU
4. Excessively use social media in the workplace
5. Shall not represent explicitly or implicitly the University on any social media platform without explicit authorization from the University

4.8 Use of Cloud Services

A risk assessment is necessary prior to the use of public cloud-based IT services to conduct QU business. The IT Services Department can assist in conducting such assessments and will provide the appropriate guidance after considering compliance, security and operational risks.

4.9 Use of Central File Storage (File Shares)

Users of the shared file storage services must comply with the following:

Departmental Shares

1. Departments are responsible for the access authorization and for the content of their assigned shared folders.
2. Departmental shares must undergo periodic reviews to ensure that the content is valid and that access control is properly set. The IT Services department can assist in such tasks but cannot be held responsible for any unexpected findings.
3. Departmental shares should not be used to back up individual user documents.
4. Access to departmental shares is restricted to devices managed by QU, i.e. personal computers may not be used to access such shares.

Individual Shares

1. Users of individual shares must not store any illegal or inappropriate content.
2. To ensure the security of the content stored in individual shares should back up their content to off-line storage devices. The IT Services department cannot guarantee that such content is backed up to central backup facilities.

4.10 Use of QU Web Services

1. Users and web site owners are accountable for any content that they post on QU web servers and that is deemed inappropriate by Qatar University.
2. Data classified as Internal, Limited Access, or Restricted shall not be made available via QU web sites or portal without adequate security controls.
3. Access to the QU portal and other web services shall be terminated when a user's role expires, i.e. the user is no longer a faculty, staff or student at the University. Exceptions are allowed with proper authorization.

4.11 Use of Audiovisual and Classroom Technology

ITS deploys and manages various audiovisual (AV) and classroom technology (CT) devices and services. These resources are the sole property of QU and should be handled properly and responsibly.

1. AV/CT resources may only be used in the course of conducting QU business.
2. In general, only the faculty members are allowed to use the Smart classroom technology system. In case a student requires their use for academic purposes, he should first obtain explicit approval and authorization to do so by the department head where the class is located or by any related faculty member.
3. Users may not attempt to fix any failure of the AV/CT equipment. Instead, they should report such failures to the ITS Service Desk.
4. Users may not at any time try to dismantle and/or move any AV/CT tools without prior authorization from the IT Services Department.
5. Smart classroom technology systems are protected through a PIN code that is provided to initiate access to the tools. The users granted access to that PIN may not share it with others.
6. Students may not use Smart classroom technology systems for non-academic purposes and outside the class hours.

7. The faculty, staff and students may not at any time try to dismantle and/or move any smart classroom technology systems without clearly notifying the ITS Service Desk and obtaining written approval and authorization to do so.

4.12 Use of QU ID Card

QU ID cardholders agree to the following terms and conditions (“Card” refers to the QU ID card):

1. The Card is the property of Qatar University and is non-transferable. A cardholder may allow another person to use the card in case of disability, under the direction and supervision of the cardholder.
2. Possession of the Card by any person other than the owner is a violation of University regulations and can result disciplinary action.
3. Cardholders are required to surrender their Card when it expires, is replaced, or when their association with the University ends.
4. Cardholders must present their Card should be presented upon request by security officers and University administrators, to access campus facilities, to attend events and activities, or to obtain certain services.
5. Depending on the card issuing guidelines, a Card replacement fee applies for cards that are lost or damaged due to neglect or misuse.
6. The University is not responsible for any losses or expenses resulting from the misplacement, theft or misuse of the Card.
7. Cardholders must maintain the Card in its original form with all information clearly visible (i.e. no stickers, punched holes, etc.)
8. Cardholders cannot use the Card as collateral or security for any reason.
9. Cardholders must immediately report a lost or stolen Card to the QU Security Office.
10. If found, lost cards must be returned to the QU Security Office.

4.13 Maintenance of Clear Screen

Users are advised to keep their screen clear of any sensitive information that others may accidently get to see. High windows and/or close them when not in use.

Users shall maintain a clear screen on their desktops/laptops by:

1. Activating the screen saver on their computer
2. Configuring the screen saver to:
    a. lock the screen if the system is idle for more than 5 minutes
    b. require a password to resume operation
3. Not tampering with the screensaver settings enforced by ITS to defeat the purpose of this policy
4. Configuring a screen saver that does NOT display information of personal nature such as a family album.

4.14 Maintenance of Clear Desk

While not purely an Information Technology requirement, users are expected to exercise due care in protecting classified information by:

1. Not leaving any information (paper/books/ledgers) being entered into the system unattended if moving away from the desk even for a short while – like attending a phone call, lunch or break hours etc.
2. Keeping restricted and limited access information protected while entertaining visitors at their desk.

4.15 Expectation of Privacy

While Qatar University does not generally monitor or limit the content of information transmitted on its network, it reserves the right to access and review such information under certain conditions. These include:

1. Responding to legal or regulatory requirements
2. Providing information required in the course of legal investigations
3. Investigating security incidents
4. Granting access to an employee's email and files that may be required for conducting QU business (e.g. email content of employees who no longer work at the University).

In some of these cases, the University may NOT notify the end users of the disclosure of their information.

4.16 Compliance

Users of QU IT Resources must:

1. Abide by all local and applicable laws, regulations and policies such as the Qatar Cybercrimes Law (Law 14 of 2014).
2. Abide by all copyright laws and licenses related to all forms of digital resources such as software, multimedia resources and licenses digital content.
3. Not use, copy, or distributed copyrighted works including, but not limited to, web page graphics, multimedia files, trademarks, software or logos unless they have a legal right to such use, copy or distribution.

Failure to comply with this policy may result in disciplinary action as per the QU policies and procedures.

1. Termination of access to resources provided by Qatar University, including access to wired and wireless network infrastructure;
2. Disciplinary and/or legal action as per QU policies and procedures and relevant local laws and regulations.