IT Policy for Staff & Faculty

DOCUMENT CONTROL

DOCUMENT NAME	IT Policy for Staff & Faculty
ABSTRACT	IT Policy applicable to all university staff & faculty
Owner	IT Department, Ashoka University
Co-owners	
Distribution List	Faculty and Staff of Ashoka University and IFRE
Linked (Related) docs	Ashoka University Mass email and Anti-Spam Policy.

DOCUMENT INFORMATION

VERSION	REMARKS
1.0	Effective From: July 2017
2.0	Effective From: July 01, 2021
Approved By	Registrar, Ashoka University

IT Policy may be amended or augmented from time to time to reflect changes in emailing and other IT services provided by the University. For any clarifications, please write to: systems@ashoka.edu.in

Any such change(s) shall be intimated to the faculty and staff by appropriate electronic communication.

TABLE OF CONTENTS

IT Policy for Staff & Faculty

Scope

This policy applies to all staff members, faculty members, contractors, visiting officials and consultants (hereby referred to as "Ashoka Users"), for the use of all IT software and systems. This includes, but is not limited to, systems, networks, facilities provided by ITS, as well as facilities provided by individual schools, departments and university laboratories, if any.

It also holds applicable with respect to access and responsibility to university information. University information is all information generated or acquired in digital form by Ashoka University.

Statement & Purpose

Individuals who engage in any Ashoka activity or who are authorized to enter the Ashoka work environment, including all visitors, must comply with all these requirements in accordance with other applicable laws, standards, and University policies.

This policy is intended

- To ensure that all Ashoka IT Systems are used only for their intended purposes
- To ensure the integrity, reliability, availability, and performance of Ashoka IT Systems
- To ensure that use of Ashoka IT Systems is consistent with the principles and values that govern use of university facilities and services

This Policy is established to promote a safe university environment and to ensure that the university fulfills its legal and external sponsor obligations.

With this IT policy in place, Ashoka University aspires to ensure that the Ashoka community can effectively communicate and exchange mission-critical messages amongst each other. The policy also aims to facilitate easier information sharing within the community; information that is relevant and adheres to the vision and mission of Ashoka University.

IT Assets

Ashoka University has made, and continues to make, considerable investment into the IT infrastructure and systems (IT assets) that are used by staff, students, and faculty members. These IT assets hold and convey important information, sometimes personal information that may be confidential and sensitive in nature.

The university is committed to managing its technology related hardware and software throughout their lifecycle. However, all users of Ashoka's IT assets are responsible for protecting the university's IT assets assigned to them. IT services will be responsible for their acquisition, maintenance, storage and/or disposal.

The following sections detailed here will explain the overall framework for the management of IT assets, starting from their acquisition to their disposal. The purpose is to specify accurate records of the IT assets and define the roles and responsibilities that are related to their proper use. It is therefore important that all IT assets are appropriately managed from the time of their acquisition to the time of their disposal, to ensure that all such IT assets deliver best value and services and also, appropriately protect the information that passes and is conveyed through them.

- **Ashoka Email ID**

Email is one of the most effective ways to communicate with a specific group of students, classrooms, staff, and other inter-departmental teams. The Ashoka email ID is a unique identifier for an individual and is assigned to staff and faculty at the time of their joining by the IT team with approval from the Human Resources (HR) department. Individuals are assigned only one personal email ID during their employment with the university and the email ID, and its associated data are deleted (and or suspended) once an employee leaves the University. In exceptional circumstances, access to an Ashoka email ID may be retained to transfer and/or recover critical information assets after approval from the relieving manager and/or Head of the Department.

- **Email Groups/ Distribution Lists**

Email Groups (or Distribution Lists) are university owned IT assets that can be used by staff and faculty to effectively communicate with their departmental teams and other groups at the university. All staff and faculty are added to the administrative user groups of the university as defined by the Ashoka University's mass email and Anti-spam Policy. The use of email groups/distribution lists enables quick and timely delivery of information to its intended recipients.

Ashoka University encourages the community to adhere to the following principles in relation to their use of emails and email groups:

- **Promote best practices in electronic communication** - Emails should not be obscene or harassing in nature. They should not use offensive language. They must not represent any fake identity of the sender.
- **Reduce the distraction from excessive mass emails and spams** - Emails should not be sent as chain letters or broadcast indiscriminately to large numbers of individuals.
- **Preserve emails as a sustainable channel for critical communication** – Reject and discourage unauthorized mass emails, if not relevant. In general, the mails should be directed only to those who have indicated a willingness to receive such emails.

This section outlines guidelines and procedures involved in the authorization and distribution of emails.

- Ashoka university maintains email groups for easy access to any team at Ashoka.
- New email groups may be requested by users after approval from the respective office mentioned below for the target members in the group.

University Stakeholders	**Approving Authority**
Academic Staff, Academic Departments, Faculty, Research Centers	Dean of Faculty/Head of the Department
Non-Academic Staff	Human Resources/Head of the Department
Student Groups	Office of Academic Affairs/Dean of academic program

Alumni Groups	Alumni Relations Office.

- Once the request is approved, the requester shall forward the request along with the related approvals to the IT department.
- It is the responsibility of the requester to write to the IT department whenever there is a need to
    - Add member
    - Remove member
    - Delete/Rename the group
- It is the responsibility of the requester to check the group membership from time to time to ensure that the member list is up to date
- It is the responsibility of all group members to adhere to the guiding principles of the email mass communication and Anti-spam policy.

- **Laptop/Desktop/Tablets/Smart Devices**

The university provides laptops/desktops for faculty and staff usage. This policy applies to all faculty and staff who use a university-owned laptop/desktop. Laptops are provided for the sole purpose of enabling employees to work outside of the confines of the workstation and/or office as an alternative to desktop.

Laptops are an option for employees whose jobs require regular mobility within/outside of the campus environment or are involved in off-campus work environments. In general practice, users are not permitted to have two University-owned computers assigned to them personally. Exceptions will be rare and made on a case-by-case basis.

- **Mobile SIM**

Some of the university employees use mobile technology as a means of sending and receiving university email, synchronizing calendars and contacts, transmitting text messages, and connecting to the internet. The purpose of this policy is to describe the conditions under which the university permits the use of mobile devices for its employees.

This section is applicable to all members of the university who hold any mobile SIM purchased by the university. These (university owned) SIMs are generally used in the employees' personal devices.

- It is critical for such employees' to not violate any policy by the university and any law of the land while using these SIM cards.
- University provided SIMs, voice plans, data plans and/or records are the sole property of the university.
- University owned SIM(s) must be returned to the university at the time of exit.

The university recognizes and enables employees to connect personally owned devices to the university's resources for accessing and synchronizing email data, contacts, and calendar information. However, these devices too must comply with the university's policies and government laws.

Password Guidelines

The Ashoka ID and password are the credentials to the campus network, sensitive information (salary and academic) and access to all the resources (academic journals, library database) and other services facilitated by IT.

The most important email ID maintenance task is choosing and maintaining a strong password. The password must adhere to the following rules:

- 11 characters
- at least one alphabet and
- at least one numeric digit
- at least one special character (#, $, @, etc.)
- The user account will get locked if 4 unsuccessful passwords are attempted

Software Licensing

The improper installation, use, or duplication of software may create legal liability for the university and its users. This section provides directions regarding the acquisition, use, distribution, and redistribution of software licenses.

It is the responsibility of each individual user to be aware of the software license restrictions for the software that they use. Use of illegal or improperly licensed software on university systems is prohibited.

Ashoka is a software licensing compliant university. Strict adherence to this policy is imperative.

- Users are strictly advised not to indulge in software piracy or breach the software licensing policy by any means.
- Users are strongly advised to own and use licensed software for personal and official use.
- The university reserves the right to scan laptops of users to detect any unauthorized software/contents being installed and/or used on any device that may be potentially harmful to the university's IT environment.
- Any violations that are brought to the notice of IT by product vendors/third parties will be taken most seriously and disciplinary action may be taken by the university, as deemed fit.

Virus & Malware

Antivirus software provides essential protection for your computer against virus infection and infiltration by other malicious software.

Malicious software, or Malware, is any software that disrupts computer operation, gathers sensitive information, or gains access to private computer systems. It can appear in the form of executable code, scripts, active content, and other software. 'Malware' could be in both forms, harmful (malicious) malware and unintentionally harmful software.

Personal vigilance and protective tools are the only way to protect oneself from these viruses.

Prerequisite & Actionable items

- All computers attached to the Ashoka university network must have a standard, supported anti-virus software installed.
- This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.
- If need be, a licensed copy of the anti-virus software can be obtained from the IT Helpdesk. The most current available version of the software will be default standard.
- The IT department reserves the right to disable access of any laptop/computer to the Ashoka university network if antivirus software is not installed on the same.
- Any activity(s) with the intention to create and/or distribute malicious programs onto university networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited, condemned, and qualify for a strict action.
- If any user receives a virus threat and/or suspects that a computer is infected with a virus, it must be reported to the IT department by writing at it.helpdesk@ashoka.edu.in, preferably with the following information, if possible: virus name, extent of infection, source of virus, and potential recipients of the infected material.
- Any computer that is suspected to be virus-infected will be removed from the network until it is verified as virus-free.
- Desktops/laptops that are connected to Ashoka antivirus server will get patch updates from the central server as required and applicable.
- Scheduled scans for network security may also be initiated at the discretion of IT and the user may not be able to stop the process.
- The antivirus program identifies all content with known virus signatures and repairs the infected files. In case a file is irreparably infected, it may be deleted. Details of such repairs and/or deletions can be viewed from the anti-virus log.

Guidelines for Virus prevention

- Always run the standard anti-virus software provided by the university.
- Never open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source.
- Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link.
- Do not click on a link sent to you if you were not expecting a specific link.
- Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
- If instructed to delete email messages believed to contain a virus, ensure to also delete the message from your deleted items or trash folder.
- Back up critical data and systems configurations on a regular basis and store backups in a safe place.

Legality and legitimacy

All issues arising out of improper software licensing and piracy that may raise concerns related to legitimacy and other related legal aspects on the following will be entirely the responsibility of the user and shall not rest with the university. These include:

- Software used by users that are not provided by Ashoka university.
- Websites and content browsed by the users within the university campus.
- Downloading & installing pirated/copyrights materials/software.
- Content or data being generated and published by the users.

Additionally, all users of university

- Must not violate any law, policy, or IT act of the Government of India.
- Must not interfere with the performance of the university.

Network and Web Access

Ashoka University endeavors to provide all staff and students with a modern, fully networked computing and IT environment for all users. The IT facilities may be used for teaching and learning experience, boost academic productivity, and minimize manual operations.

- **Guidelines**
  - The access to Internet and Intranet resources is limited to 2 devices for staff and 5 devices for faculty. However, faculty can reach out to the IT department for any exceptions in the number of devices.
  - Users are expected to use only their official/Ashoka email ID for official communication with other members of the University.
  - Email & other network communication facilities must not be used to harass, offend, or annoy other users of the university by any means.
  - Users must not send emails or messages masquerading as another user.
  - Spamming, commercial advertisements or solicitations are strictly prohibited.
- **Restrictions**
  - P2P (applications like torrent etc.) and other unsafe websites shall not be accessible. All users are expected to practice discipline in this regard. Users violating this clause may be liable to strict disciplinary action and/or penalty.
  - Websites unsafe for the university's network are currently blocked. Review of such websites will be based on deliberation with the management.
  - High bandwidth consuming categories (e.g., video streaming, on-line music, games etc.) will be contained or blocked, if it hinders other online activities of the University, such as learning management systems, admissions, events, skype sessions and video conferences etc.

Information Access & Security

Any information stored on the IT systems of Ashoka university is the property of the university and users cannot claim any privacy requirements of such information.

The objective of this section is to ensure protection of university's information systems against damage, destruction and/or unauthorized changes or disclosure, whether intentional or unintentional. University information should be used only for appropriate university purposes. All members of the university community should be aware of their obligations to protect university information. In particular:

- University information should only be accessed by persons when they are performing activities and responsibilities associated with their university position.
- University information may only be disclosed to individuals where need exists, and the individual has appropriate authorization.
- Those authorized to access university information are responsible for securing it from any unauthorized access.
- Those authorized to grant or revoke access to university information (as specified in section below) are responsible for following procedures to ensure that access is appropriately assigned, modified as needed, and cancelled promptly as and when required.
- Misuse of university information will be regarded with the utmost seriousness. Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures of the University.

Authorization to grant or revoke access to University Information:

Type of Information	**Official Authorized to grant or revoke access**
Academic and Educational Information	Office of Academic Affairs
Financial information	Head of Department, Finance
Purchasing information	Head of Department, Purchase
Budget information	Head of Department, Finance
Human Resources information	Head of Department, Human Resources
Student information	University Registrar

- **Guiding Principles**

  Ashoka university information security program is based on the following principles:

  - **Confidentiality**: Protection of information by ensuring that information is accessible only to the authorized personnel.
  - **Integrity**: Assuring the accuracy and completeness of information and its associated information

processing methods. Maintaining the data in its correct state and preventing it from being modified, whether intentionally or unintentionally.

  - **Availability**: A subset of Confidentiality and Integrity. Ensuring that information and associated assets or systems are available to the authorized users when required.
  - **Accountability** (non-repudiation): Ensuring that the users are fully accountable for their actions on the Information Systems.

- **Statements**
  - University provided devices (Laptop, Desktop, Mobile etc.) are property of the university. These devices present an increased level of risk to both the user and the institution.
  - In requesting and accepting, all or any of these devices from the university, users acknowledge and accept this risk and agree to make every attempt to minimize/reduce the risk.
  - The user must not physically alter or make any irreversible changes to these devices.
  - Should a laptop be damaged beyond repair, lost, or stolen it becomes the responsibility of the user to pay for the replacement/repair.
  - The user must not attempt to repair or alter any part of these devices unless explicitly instructed to do so by the IT department.
  - In cases where repairs are not considered cost effective, requisition for a new device can be made. However, it will have to be through the budgeting process of the University.
  - Upon leaving the university's employ the employee will return these devices to the IT department on or before their final day.
  - All university-owned laptops are put on a refresh cycle. After a laptop has been in use for four years it will be evaluated and replaced, if deemed unfit for use.
- **Responsibility of the User**
  - IT assets shall be protected against physical or financial loss whether by theft, mis-handling or accidental damage either through primary prevention (e.g., physical security) or remediation.
  - Each user is responsible for the security of the university-owned laptop and the data contained therein, regardless of whether the laptop is used in an office, at one's place of residence, or in any other location such as a hotel, conference room, car or airport etc.
  - Laptops are intended to be used solely by the employee and should not be shared with family, friends, or other employees.
  - Loss or theft of IT equipment must be reported immediately to the IT Department
  - All IT equipment (including home working) must be returned to the relevant IT support team upon replacement, equipment redundancy (i.e., no longer required for university business). Equipment holders will be responsible for any equipment issued to them until it has been returned safely to the IT Services for redeployment or disposal.
  - All IT assets should be available or made available for audits throughout their lifecycle.
  - Fixed IT equipment must not be moved without the consultation of IT Services and an update of

asset data must be made.

  - Any equipment that is not operating normally must be immediately returned to the IT support team.
  - Information about all IT assets shall be held in an IT Asset register that enables them to be tracked, managed, and audited throughout their lifecycle.

- **Responsibility of the IT Department**
  - The IT Department will provide the software(s) as applicable for devices like laptop and desktop.
  - The IT Team will provide full support for all uses of the laptop at on-campus environments.
  - Limited support will be provided for off-campus environments, e.g., for external factors such as problems with the employee's home ISP.
  - The IT team will be solely responsible for the use and/or functionality of software(s) installed by IT.
- **Disposal**
  - Disposal of firm assets, including the sale, transfer, donation, write off or sustainable disposal (recycling), is done in adherence with government regulations. Computer hardware must have all software and information securely removed prior to their disposal.
  - Highly sensitive data must be deleted using secure methods as soon as they are no longer required.
  - This will be done in sync with the Accounts/Finance department.

Policy Review

This policy may be periodically reviewed and modified by the respective Department Head(s), who may consult with relevant committees, faculty members, students, and/or staff of the University.

The latest version of the policy will be always available on MyAshoka (See: https://my.ashoka.edu.in) and is subject to change during the periodic policy review undertaken by the University. Please visit the MyAshoka Portal to review the latest up to date IT policy.