

IT POLICY FOR FACULTY MEMBERS

Upon joining, all full-time faculty members are provided with the following facilities

- ULAB domain email
- Individual computer with necessary accessories and Internet connection.
- Access to URMS with necessary features.
- Access to Wi-Fi network on both campuses
- Access to ULAB File Server
- ULAB IT Helpdesk support.

Email address creation

- First try to use the ‘First.Last’ legal name to create the account but there are several conditions that may impact:
 - I. If the derived First.Last account name is already in use,
 - II Try appending the Middle name as Last name –or-try appending a sequence number at the end of the Last name (if Middle is Missing, or already taken)
- Display name (Full name) will be used as per HR naming policy
- The template will be followed for creating Email signature.

On Leave (longer than 3 months)

- 1 In the case official leave (e.g. study leave, maternity leave, extra ordinary leave, etc.), access to the following ULAB IT facilities will be closed from the first day of leave:
 - ULAB File Server
 - Campus Wi-Fi,
 - URMS
- 2 On-leave faculty members must return the officially allocated computer and IT accessories to ULAB IT
- 3 If a faculty member does not re-join ULAB on the expiration of the leave, access to the following ULAB IT facilities will be closed immediately:
 - ULAB email
 - ULAB email groups

Resignation/Termination/Discontinuation

- 1 Access to the following ULAB IT facilities will be closed immediately:
 - ULAB domain with computer
 - ULAB File Server
 - Campus Wi-Fi
 - URMS
 - ULAB email groups
- 2 Access to ULAB email will be closed after 21 days from the effective date of resignation/discontinuation.
- The university reserves the right to extend or curtail this time frame on a case by case basis.
- 3 Faculty members must return the officially allocated computer and IT accessories to ULAB IT

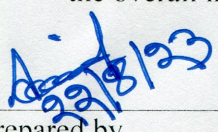
N.B.. Common IT policy will be applicable for all faculty members.

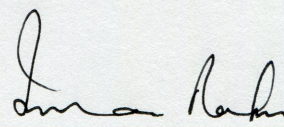
**COMMON IT POLICY
FOR FACULTY AND ADMIN MEMBERS**

- 1 Computers will be allocated as per following
 - a. Desktop All faculty and admin members from Assistant Officer and above.
 - b. Laptop Assistant Manager and above (pursuant to Laptop policy)
- 2 Laptop policy
 - a. Laptops will be available only to faculty or admin members who have a demonstrated need for mobility
 - b. No one whose work mainly concerns handling sensitive and confidential university or student data will be issued a laptop
 - c. Laptop users may carry their laptop to their residence but they will be responsible for any kind of damage, theft or loss, data security, data privacy, etc through signing on undertaking.
- 3 CCTV Following officials will have the access to the CCTV
 - a. Vice-Chancellor
 - b. Registrar
 - c. Proctor
 - d. HoD/Manager, ITD
 - e. HoD/Admin
 - f. Security in charge

REGULATIONS

- 1 All users must protect their computers with passwords.
- 2 Users will not allow others to share their computer/email/URMS/Wi-Fi access or any kind of password and will ensure their computers are used only by themselves.
- 3 Administrative password control of all computers will be restricted by the ULAB IT
- 4 Every one using a laptop and/or mobile device(s) - including personal devices - to access the campus Wi-Fi must register her or his device(s) with ULAB IT
- 5 Users will ensure the computers including UPS, printer, speaker, scanner, etc. are switched off before leaving the office.
6. Users will be responsible for proper maintenance including cleanliness of the computer and its accessories.
- 7 All concerned will be careful in using all IT facilities including computers, turnstiles and other electronic devices in order to obtain maximum utility
- 8 Any lost/damage of IT resources while in position of an individual to be made good by the individual concern.
- 9 In the case of theft, a GD must be filed with the local Thana and inform to ULAB authority within 24 hours
- 10 No one may use any IT facilities to commit any crime or break the ULAB Code of Conduct, including (but not limited to):Cybercrime, cyber-bullying, sexual harassment, threats, intimidation, theft, identity theft, phishing, hacking, piracy, spam, viruses, terrorism or pornography (See also ULAB Code of Conduct.)
- 11 ULAB authority reserves the right to block any Internet sites or allow restricted access and amend any provision of this policy or to add/delete any of provisions any time for the overall interest of ULAB


Prepared by
Md Arif Billah Al-Mamun
Senior Assistant Manager
In Charge of IT


Approved by
Professor Imran Rahman
Vice Chancellor