



Bring Your Own Devices (BYOD) Policy Ver-1.0

Delhi Skills & Entrepreneurship University (DSEU). All rights reserved.

This document is meant for exclusive use of DSEU. No part of the document may be copied, reproduced, stored in any retrieval system, or transmitted in any form or by any means, electronically, mechanically, or otherwise without the prior written permission from Registrar-DSEU.

Release Control

Release Date	Version No:	Details	Released by:	Approved by:
October 19, 2021	V 0.1	Pre-release, the purpose of pre-release is to inform all stake holders about the issuance of this policy and also to give advance intimation to the assured departments to get prepared.	Mr. Joyjit Roy Ghatak Choudhury, Consultant (IT) - DSEU Mr. Prasun Kumar Assistant Registrar (IT)-DSEU	
November 17, 2021	V 1.0	First release	Mr. Ashwani Kansal, Registrar - DSEU	Dr. Neharika Vohra, Vice Chancellor- DSEU

Policy Owner

Department:	Represented by:	Date
Registrar-DSEU	Mr. Ashwani Kansal	November 17, 2021

Policy assured by:

Department:	Represented by:	Applicable to	Date
Directors / HODs	Individual Role Holders	Respective users using computing assets.	November 17, 2021

Delhi Skills & Entrepreneurship University (DSEU). All rights reserved.

This document is meant for exclusive use of DSEU. No part of the document may be copied, reproduced, stored in any retrieval system, or transmitted in any form or by any means, electronically, mechanically, or otherwise without the prior written permission from Registrar-DSEU.

Table of Contents

1. OBJECTIVE	4
2. SCOPE	4
3. DEFINITIONS	4
4. POLICY DETAILS	5
4.1. DEVICES AND SUPPORT	5
4.2. USERS RIGHTS AND RESPONSIBILITIES	6
4.3. UNACCEPTABLE USE	7
4.4. ADHERENCE WITH CENTRAL, STATE, LOCAL, CYBER AND APPLICABLE INTERNATIONAL LAWS	7
4.5. VIOLATION OF POLICY	8
4.6. ENFORCEMENT AND COMPLIANCE	8

Delhi Skills & Entrepreneurship University (DSEU). All rights reserved.

This document is meant for exclusive use of DSEU. No part of the document may be copied, reproduced, stored in any retrieval system, or transmitted in any form or by any means, electronically, mechanically, or otherwise without the prior written permission from Registrar-DSEU.

1. OBJECTIVE

This policy outlines the Delhi Skill & Entrepreneurship University's (DSEU) approach to use of mobile devices and 'Bring Your Own Device' (BYOD).

BYOD shall be taken to mean any device used to access DSEU resources and Information Technology Systems that is either not owned by DSEU or is not managed centrally by the University.

In response to an increase in personally owned devices being used in the work environment, DSEU has established an official BYOD policy.

BYOD is the act of using a personal computing device (computer, tablet, phone, etc.) for education related or personal activities while at the university. DESU users while using their personal devices must abide by the policy below.

The purpose of this policy is to set out the controls when using mobile devices (phones, pads, laptops etc) and mitigate the following risks:

- Loss or theft of mobile devices, including the data on them
- Compromise of classified information through observation by the public
- Introduction of viruses and malware to the network
- Damage to reputation of the user and/or the university
- Safeguard the University's information from security threats that could have an adverse effect on its operations or reputation.
- Fulfil the University's duty of care toward the information with which it has been entrusted.
- Protect the confidentiality, integrity, availability and value of information through the optimal use of controls.

It is important that the controls set out in this policy are observed at all times in the use and transport of mobile devices.

2. SCOPE

This policy applies to all DSEU members (employee, students, guests, contractual third parties and any other authorized persons) who have access to DSEU information systems and other relevant IT-based resources and any other user who utilizes the network or computing resources provided by DSEU for education, work or personal activities with a personally owned device such as:

- Portable computers; e.g.; laptops, notebooks, netbooks
- Portable storage media; e.g.; USB storage devices, flash memory cards, CD/DVD ROM

Delhi Skills & Entrepreneurship University (DSEU). All rights reserved.

This document is meant for exclusive use of DSEU. No part of the document may be copied, reproduced, stored in any retrieval system, or transmitted in any form or by any means, electronically, mechanically, or otherwise without the prior written permission from Registrar-DSEU.

- Mobile devices; e.g.; cellular smartphones, tablet computers

3. DEFINITIONS

Processing data - means obtaining, recording, holding, sharing, and retaining and deleting of University data.

BYOD (Bring Your Own Device) – the use of personally owned devices to undertake University work or to process University Data.

Personally owned devices - Include - but is not limited to – laptops, personal computers, netbooks, tablets and smartphones that are used to collect, store, access, transmit, carry, use or hold any University data. It applies to the use of the Personally Owned Device both during and outside of normal working hours and whether or not it is used at your normal place of work.

High Risk Data - High risk personal data or sensitive information) and including any other information which is identified as being of a confidential or proprietary nature.

Computing Resources: All DSEU's information processing resources including owned, licensed, or managed computing services, hardware, software, and use of DSEU's network via physical or wireless connection regardless of the ownership of the computer or device connected to the network.

University Community: Includes faculty, administrators, staff, student workers, graduate/technical assistants, alumni, interns, guests or agents of the administration, external individuals and organizations accessing DSEU's network services, and other authorized users.

4. POLICY DETAILS

Mobile devices such as smartphones, laptops, and tablets that are not provided by The University are required to meet minimum controls to protect University data.

4.1. DEVICES AND SUPPORT

All devices connected to the DSEU network are required to adhere to the Acceptable Use Policy for IT Resources.

Devices must be registered under the users account and be updated on all software patches and anti-virus solutions. IT Services may, without notification, prevent or ban any personally owned device which disrupts any University Computing resource or are used in a manner which violates any University policy.

Technical support for personally owned computing devices is limited to the following:

- Troubleshooting network connection issues while on the campus network.

Delhi Skills & Entrepreneurship University (DSEU). All rights reserved.

This document is meant for exclusive use of DSEU. No part of the document may be copied, reproduced, stored in any retrieval system, or transmitted in any form or by any means, electronically, mechanically, or otherwise without the prior written permission from Registrar-DSEU.

- Troubleshooting and installation of approved University software resources.
- Configuration of email clients for connection to the email system.
- Configuration of the SSL VPN client to allow access to secure resources with approval.
- Providing software application support if the software is required to perform job functions as determined by the Information Technology department.

Note: It is the responsibility of the device owner to have and provide authentic, individually owned and registered software before assistance is provided.

Examples of support services that will not be provided, but is not limited to:

- Troubleshooting device performance or hardware problems
- Installation of new or replacement hardware
- Troubleshooting software applications or cloud services
- Installing operating system updates, patches or software applications not required for job functions
- Backing up device data or migration to another device
- Third party email clients/accounts
- Removal of malware, spyware or virus

4.2. USER RIGHTS AND RESPONSIBILITIES

Users to ensure that

- Their use of personally owned devices is in line with University requirements to ensure data security and the protection of University owned intellectual property and confidential information.
- No unauthorized persons are able to access University owned data on their personally owned devices.
- University data is removed from the device before disposing of the device or selling it or passing onto another individual.
- You are responsible for all traffic originating from your networked devices whether you generate the traffic, or not.
- You are responsible for abiding by all applicable laws set forth by Central, State and Local Governments.
- You are responsible for protecting your privacy.
- You are responsible for not violating the privacy of others.
- You are responsible for keeping your network devices up to date with current security patches.
- You are responsible for using anti-virus software and ensuring that such software is at the most current release & patches updated.
- You are responsible for protecting any and all sensitive data for which you have access to.

Delhi Skills & Entrepreneurship University (DSEU). All rights reserved.

This document is meant for exclusive use of DSEU. No part of the document may be copied, reproduced, stored in any retrieval system, or transmitted in any form or by any means, electronically, mechanically, or otherwise without the prior written permission from Registrar-DSEU.

- You are responsible for following all applicable university policies relating to your use of Information Technology resources. These policies may be viewed in our website "IT Policy"
- You are responsible for ensuring the security of Information Technology resources under your direct control.
- You are responsible for securing your granted access privileges and passwords for Information Technology resources.

4.3 UNACCEPTABLE USE

The use of the service for the following activities is prohibited:

Inappropriate use of the network is not permitted. This policy does not enumerate all possible inappropriate uses but rather presents some guidelines (listed below) that the DSEU may at any time add or reasonably determine that a particular use is inappropriate.

- Spamming and invasion of privacy of others, Violating intellectual property law, Transmitting obscene or indecent speech or materials, Transmitting defamatory or abusive language, Hacking or distribution of internet viruses, Worms, Trojan horses, or Other destructive activities.
- Not respecting the privacy and intellectual property rights of others.
- Not respecting the integrity of DSEU's network and any other public or private computing and network systems.
- Use of the Network for malicious, fraudulent, illegal or misrepresentative purposes.
- The Network used in a manner that precludes or hampers other users access to the network or other any other networks.
- Installation or use that modifies, disrupts, or interferes in any way with service for any user, host, or network.

4.4. ADHERENCE WITH CENTRAL, STATE , LOCAL, CYBER AND APPLICABLE INTERNATIONAL LAWS

As a member of the DSEU community, you are expected to uphold local acts/ordinances and central, state, cyber and applicable international laws. DSEU's guidelines related to use of technologies derived from this concern, including laws regarding license, copyright and the protection of intellectual property.

As a user of DSEU's computing and network resources you must:

- Abide by all Central, State, Local, Cyber Law and applicable International Laws.
- Abide by all applicable copyright laws and licenses.
- DSEU has entered into legal agreements or contracts for many of our software and network resources which require each individual using them to comply with those agreements.

Delhi Skills & Entrepreneurship University (DSEU). All rights reserved.

This document is meant for exclusive use of DSEU. No part of the document may be copied, reproduced, stored in any retrieval system, or transmitted in any form or by any means, electronically, mechanically, or otherwise without the prior written permission from Registrar-DSEU.

4.5. VIOLATION OF POLICY

If it is suspected that this policy is not being followed, please report the incident to abuseinfo@dseu.ac.in

Loss of devices holding University data may cause damage and distress to those who entrust us to look after their data, damage the University's reputation and its relationship with its stakeholders (including research funders), and have significant legal and financial consequences.

Loss of devices containing other University data may give rise to loss of rights in intellectual property, inability to register rights in intellectual property and breach of contractual and other obligations to third parties for disseminating or otherwise failing to protect confidential information.

Thus ensuring that you keep your devices safely and also never share your personal device with a relative or a friend.

Failure to comply with this policy may result in us revoking your access to the University's systems, whether through a device or otherwise. It may also result in disciplinary action being taken against employees up to and including dismissal. In the case of breach of this policy by a contractor, worker or volunteer, it may lead to the termination of their engagement. This will apply whether the breach occurs during or outside normal working hours and whether or not use of the device takes place at your normal place of work. You are required to co-operate with any investigation into a suspected breach, which may include providing us with access to the device.

This policy will not supersede any DSEU developed policies but may introduce more stringent requirements than the university policy. Any exceptions to this policy must be approved in advance by DSEU IT Team.

4.6. ENFORCEMENT AND COMPLIANCE

Heads of Schools, Functions and Departments to ensure that

- That their staffs are made aware of this policy and that breaches of it are dealt with appropriately.

Registrar – would be in-charge of implementation, monitoring and review of this policy

If any user is found to have breached this policy, they may be subjected to DSEU's disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from DSEU IT Team.

Delhi Skills & Entrepreneurship University (DSEU). All rights reserved.

This document is meant for exclusive use of DSEU. No part of the document may be copied, reproduced, stored in any retrieval system, or transmitted in any form or by any means, electronically, mechanically, or otherwise without the prior written permission from Registrar-DSEU.