अमर उजाला
हर सवेरे नया जोश
नया उजाला

BYOD – Policy

(Bring Your Own Device)

Ver 1.0

Table of Contents

1. Overview

Authorized employees and third parties may wish to use their Smart phones/Tablets for work purposes. Bring your own device (BYOD) is an IT policy where employees are allowed or encouraged to use their personal mobile devices/tablets to access enterprise email and data.

2. Purpose

The purpose of this policy is to ensure the proper usage of Amar Ujala's Email and data and make users aware of what Amar Ujala deems as acceptable and unacceptable use of its email system.

3. Scope

This policy is particularly relevant to employees who wish to use Smart devices (Smartphone's and Tablets) for work purposes. This policy also applies to third parties acting in a similar capacity to our employees whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with our information security policies.

4. Policy

4.1 BYOD is allowed into Amar Ujala's network upon prior business approval from the respective Directors.

4.2 IT will facilitate in configuring the official email ID of Amar Ujala on the Smart phones/Tablets.

4.3 IT Help/Service Desk is responsible for providing limited support for BYOD on a 'best endeavors' basis for work-related issues only. Information security incidents affecting Smart Phones/Tablets used for BYOD should be reported promptly to IT Help/Service Desk in the normal way.

4.4 IT will not directly entertain the hardware related issues without the prior approval of Corporate Functional Head and the final authorizer would be IT CFH

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team of IT will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, remote monitoring, business tool reports, internal and external audits, and provide feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team of IT in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action as per Amar Ujala's policy

6. Definitions and Terms

7. Revision History

Date of Change	Responsible	Summary of Change
Nov 2014	IT Helpdesk Team	