DIGITAL USE AND BIOMETRIC POLICY FOR S' RESIDENCES RESIDENTS

Purpose and Scope:

This policy outlines the rules and expectations regarding the use of digital infrastructure, including biometric systems, smart access, and app-based services at S' Residences. It ensures accountability, operational efficiency, and the safety of all residents through responsible use of technology.

Biometric and Smart Access System:

1.1. All residents are required to use biometric authentication (fingerprint or facial recognition) or smart access cards to:

- Enter or exit the premises via turnstiles, Record attendance and outpass movement
- Access meals at the dining hall (meal tapping), Use certain restricted common areas (gym, quiet study room, etc.)

1.2. Biometric access ensures real-time monitoring for the safety of residents and helps track unauthorised movement.

1.3. Entry or exit without biometric tapping, including tailgating, will be treated as a policy violation and recorded accordingly.

1.4. Under no circumstances should residents share or swap access cards with others. Doing so will result in disciplinary action.

Use of the S' Residences Mobile Application:

2.1. The official mobile app is mandatory for all residents to:

- Apply for gate passes, emergency leave, and late return requests, Submit maintenance and facility complaints
- View weekly dining menus, Track personal attendance and movement logs
- Receive campus notices and housing-related updates

2.2. The app must be kept updated for uninterrupted access to services.

2.3. Misuse or unauthorised attempts to alter app data will lead to loss of privileges and possible escalation to IT administrators.

System Maintenance and Support:

3.1. Residents must immediately report issues related to biometric devices or mobile app malfunctions to the hostel administration or IT support.

3.2. In case of verified medical conditions (e.g., injuries, skin conditions affecting biometric scan), temporary access exemptions may be granted by prior written approval.

3.3. Offline or manual entry will be permitted only in case of verified system failure and must be logged at the security desk.

Data Privacy and Confidentiality:

4.1. Biometric and movement data are stored securely and used only for internal monitoring, safety alerts, and academic compliance purposes.

4.2. Data will not be shared with third parties without appropriate consent, except as required by law or institutional policy.

Violations and Disciplinary Measures:

5.1. The following will be treated as violations of the digital use policy:

- Sharing of ID/access credentials, Misuse of outpass or entry logs
- Tampering with biometric or smart access devices, Unauthorized modification of digital records

5.2. Penalties for violations may include:

- Verbal/written warnings, Suspension of digital access
- Monetary fines, Expulsion in cases of data tampering or security threats

Amendments:

6.1. This policy is subject to regular review and may be updated to align with new technologies, data protection laws, or institutional needs.

By adhering to the Digital Use and Biometric Policy, residents of S' Residences help maintain a secure, accountable, and digitally enabled living environment, ensuring smoother operations and enhanced safety for all.