Guidelines for Personal Device (BYOD) Use at Kobe City University of Foreign Studies

(Purpose)

Article 1 This guideline aims to establish rules and precautions for students' use of personal devices (BYOD) at Kobe City University of Foreign Studies, in order to prevent information leaks, loss, theft, and unauthorized access, and to maintain and enhance information security.

(Scope)

Article 2 This guideline applies when students use personal devices to access information assets at the university. Specifically, it is intended for "all students who access information assets" as defined within the scope of the Kobe City Public University Corporation Information Security Policy.

(Definitions)

Article 3 "Personal device" refers to information and communication devices owned by students, such as PCs, tablets, and smartphones.

(Compliance Requirements)

Article 4 Students must comply with the following requirements when using personal devices:

1. Adhere to the contents of this guideline.
2. Always set a password and enable device locking on personal devices.
3. Keep the operating system and applications on personal devices up to date.
4. Implement appropriate antivirus measures on personal devices, such as conducting regular virus scans.
5. Use the university-provided account when accessing the university's information assets.
6. Use the university-provided email address for all email communications.
7. Take measures against theft or loss, such as not leaving devices unattended and keeping mobile devices with you at all times.

8. Take measures against visual or audio eavesdropping, such as using privacy screens or headphones.
9. In the event of theft, loss, or virus infection of a personal device, handle the situation at one's own responsibility.

(Cost Responsibility, etc.)
Article 5
1. Students are responsible for all communication, maintenance, and related costs for their personal devices.
2. Any unforeseen incidents that occur while using a personal device shall be handled at the student's own responsibility.

(Miscellaneous)
Article 6 In the event of any questions regarding the interpretation or implementation of this guideline, the Chief Information Security Officer shall make the final decision.

Supplementary Provisions
This guideline shall come into effect on April 1, 2026.