MOBILE DEVICES POLICY

Kingsridge Cleddans

HOUSING ASSOCIATION LIMITED

APPROVED	**28 March 2023**
Date of Next Review	March 2026

1. INTRODUCTION

This document details the requirements for the use and secure operation of portable mobile devices and removable media by Kingsridge Cleddans Housing Association staff. Kingsridge Cleddans Housing Association recognises the advantages of using portable / mobile devices provided for staff during the performance of their daily duties.

It is also recognised that Remote Access is a valuable method for staff to connect to the Association's network resources, when away from the Association's premises.

This document covers the use of all portable computing storage and remote access devices used for work purposes, whether they be owned by the Association or privately owned by staff (as defined below under '2. Scope') in order to:

- Provide secure access to the Association's information systems.

- Preserve the integrity, availability, and confidentiality of the Association's information and information systems.

- Manage the risk of serious financial loss, loss of customer and public confidence or other serious business impact which may result from a failure in security.

- Comply with all relevant regulatory and legislative requirements (including Data Protection laws) and to ensure that the organisation is adequately protected under computer misuse legislation.

As part of the provision of Information Management and Technology (IM&T) services to staff within the Association, staff may purchase their own portable computing equipment for use, on an ad hoc basis, on the Association's business. As such, it is essential that such devices are covered by appropriate security controls in accordance with Article 5(1)(f) of the UK General Data Protection Regulation.

2. SCOPE

This policy applies to all employees of the Association, including temporary staff, agency and locum staff, students, voluntary staff, contractors, and trainees on temporary placement, as well as those persons holding honorary positions ('staff').

3. REQUIREMENTS

3.1 Portable Devices

For the purpose of this policy, a Portable Device is defined as any device that may synchronise with another computer, and will include any of the following items:

- Laptop and notebook computers
- iPads / Tablets
- Smart phones including iPhones and any other mobile system that may fall into this category, including Blackberrys.
- Webcams
- USB memory sticks (only for temporary storage of information, information to be transferred to the secure server as soon as practicable and deleted from USB stick)
- MP3 players including iPods (must not be used at any time for storing the Association's personal or commercial information)
- CDs, DVDs
- Any other item that may be utilised to store or transport data.

This list is not exhaustive. Any portable device used in connection with the organisation must be encrypted to a minimum of 256bit encryption. Further guidance may be obtained from the Director in relation to what is defined as a portable media device and encryption.

3.2 Use of Own Devices

The use of staff members' own devices is permitted in accordance with the following guidelines:

- staff will only be allowed access to the Association's Wi-Fi network; there will be no access to the Association's secured drives;
- staff must not save/store confidential or customer identifiable information on their personal devices.
- Staff are to comply with the Association's Bring Your Own Device Policy.

3.3 Working Procedures

- All Portable Devices issued by the organisation are to be issued to a named individual and must not be shared or used by anyone who is not recorded as the asset owner for audit purposes and to comply with Data Protection legislation.
- The transfer of any Portable Device between staff members must only be done via the Director. All laptops, notebooks, USB Pens, iPads, Blackberrys and other Smartphones must be encrypted. Staff owned devices must have the password facility activated.
- Documents containing personal or commercial data from the organisation's servers must not be copied without express permission of the Director.
- Information must be protected from persons not authorised to view it.
- Whenever possible, Portable Devices should not be used in public areas.

3.4 Asset Management

Any business-related software applications on mobile Portable Devices must be approved, appropriately licensed, and recorded on the Association's licence asset register. The Association's IT partners will maintain a software application asset list to ensure licensing conditions are not breached. Procurement of additional software for business must adhere to the organisation's procedures, including the potential for a Data Protection Impact Assessment to be completed.

Portable Devices must not be readily identifiable as belonging to or associated with the Association. If the Portable Device can be associated with the Association , this may increase the impact (e.g. risk) to the Association's reputation in the event of loss or theft. However, all of the Association-owned Portable Devices must carry asset identification.

All iPads should have a Mobile device management system installed before they are issued.

Staff issued with an Association-owned encrypted Portable Device will be required to sign a declaration that they have read, understand, and accepted this policy, and the conditions of use before using the device. Where a generic Business Group device is provided, all staff having access to the device will be required to sign the declaration.

Upon leaving the Association all mobile media devices must be handed back. Failure to hand the mobile media device back at the end of your employment may be viewed as theft and may result in legal action being taken against you.

3.4 Security and Passwords

Staff are personally responsible for the security of the Portable Device wherever they may be including Association's premises, the premises of other organisations, in private or public transport or at home. Staff will be liable for any cost resulting from the loss or accidental damage of the device as a result of carelessness. Where a device has been stolen, on production of a Police Crime Report, the Association will be assume liability.

Staff must employ whatever security initiatives are available with the device, for example utilising the device PIN code. In addition to the individual Portable Device security features, each Portable Device must have a password enabled to access it.

4. LEGISLATION

This Policy has been written to meet the requirements of:

- The Computer Misuse Act 1990
- The UK General Data Protection Regulation
- The Data Protection Act 2018
- The Privacy and Electronic Communications Regulations (PECR) 2003

5. REVIEW CYCLE

This policy will be reviewed annually or as our needs and procedures change or are updated.