Kingsridge Cleddans

HOUSING ASSOCIATION LIMITED

Information Security Policy & Procedure

APPROVED	**21 May 2024**
Date of Next Review	May 2027

Introduction

Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post, or using electronic means, stored on tape or video, or spoken in conversation. It may include personal information about a living individual, or it may be required for the running of Kingsridge Cleddans Housing Association's business. Kingsridge Cleddans Housing Association is committed to ensuring that all personal data will be processed in accordance with best data security practice and the UK General Data Protection Regulation (UK GDPR).

Purpose

The purpose and objective of this Information Security Policy is to protect Kingsridge Cleddans Housing Association's information assets from all threats, whether internal or external, deliberate or accidental, to protect personal and business information, ensure business continuity and minimise business damage by ensuring that all Kingsridge Cleddans Housing Association personnel understand our requirements for handling personal data and to clarify the standards of data security which we expect to be implemented.

Information will be protected from a loss of:

- Confidentiality: ensuring that information is accessible only to authorised individuals
- Integrity: safeguarding the accuracy and completeness of information and processing methods, and
- Availability: ensuring that authorised users have access to relevant information when required

Responsibility for data security

This policy applies to all Kingsridge Cleddans Housing Association staff.

All Kingsridge Cleddans Housing Association staff have a responsibility to apply adequate security to personal data that they handle to prevent it from being unlawfully accessed, lost, wrongfully deleted or damaged and to comply with this policy. The Director of Kingsridge Cleddans Housing Association is responsible for overseeing this Information Security Policy and, as applicable, developing related policies, procedures, and guidelines.

Personal Data

Personal data means information that relates to a living individual who can be identified either from that information alone or when that information is combined with other information.

Security Measures

Kingsridge Cleddans Housing Association is committed to protecting the integrity of the information we hold. A data security breach could have a very serious legal, financial, and reputational impact on the business.

Training

Appropriate training will be made available for existing Kingsridge Cleddans Housing Association staff who have responsibility for handling personal data. Each new employee will be made aware of their obligations for data protection during their induction to the organisation. Training requirements will be reviewed on a regular basis to take account of the needs of the individual, and to ensure that Kingsridge Cleddans Housing Association staff are adequately trained.

Compliance

Compliance with this policy forms part of the employee's contract of employment and failure to comply may constitute grounds for action, under the organisation's disciplinary policy.

INFORMATION SECURITY PROCEDURES:

All Kingsridge Cleddans Housing Association staff must adhere to the following procedures to ensure security of Kingsridge Cleddans Housing Association's personal data:

Use of Hardware and systems

Our systems have been designed to enable us to work effectively and securely, and all staff are expected to use them in a professional manner by:

- Using a strong password which must contain a minimum of 8 characters and must consist of at least 1 upper case, 1 lower case and at least 1 number.
- Never sharing passwords
- Never sharing devices
- Locking screens and mobile devices when not in use and ensuring they are physically secure.
- Ensuring anti-virus is kept up to date.
- Not downloading unauthorised software or applications onto any of our hardware
- Not connecting unauthorised devices or equipment (including USB sticks, printers etc…) to our devices or systems
- Not connecting to our systems over unsecured wi-fi

Use of own devices for business purposes

Staff may not use their own personal devices for accessing our business information or undertaking work for Kingsridge Cleddans Housing Association

e-mails

- Staff shall be diligent when using email to ensure that they do not provide unauthorised access to our information, spread viruses, or infect our systems with malware.

- Staff shall not click on hyperlinks or open attachments in emails unless they know and trust the sender.

- We shall encrypt any documents containing special categories of personal data before sending by email.

- We will double check the recipients before hitting “Send”.

The company email account remains the property of Kingsridge Cleddans Housing Association and we may monitor it from time to time to ensure compliance with this and other policies.

Printing

Care must be taken when printing including;

- Ensuring staff only print documents for which they absolutely need a hard copy.
- Ensure all printing is collected from printers immediately.
- Any printing remaining on a printer at the end of the day will be shredded.

Storage of hard copy documents

Any hard copy (paper) documents containing personal data must be stored in a locked desk or cupboard with limited access. Any keys for accessing these areas must also be stored securely.

When a document containing personal data is no longer required it should be shredded. ONLY documents that do not contain personal data or sensitive information should be put in general waste or recycling bins.

Protecting Information when travelling

In addition to the measures set out above, particular care must be taken to prevent disclosure of information when out of the office. Avoid situations where others can read documents.

Clear desk

All Kingsridge Cleddans Housing Association staff are to tidy away all documents when they are away from their desk/workstation for more than a short period of time, namely at lunchtime, when attending meetings and overnight.

Documents which are likely to be needed by other members of staff should be stored in shared, locked filing cabinets. Other documents may be locked in storage the company provides individual staff members i.e., desk pedestals.

Spare keys for all desks/workstations should be available so that documents can be accessed if the staff member is absent from work.

Kingsridge Cleddans Housing Association staff should make sure that any documents lying on their desk/workstation are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Sensitive information, if needed to be printed, should be cleared from printers immediately.

Paper records which are left on desks/workstations overnight or for long periods of time are at risk of theft, unauthorised disclosure, and damage. By ensuring that Kingsridge Cleddans Housing Association staff securely lock away all papers at the end of the day, when they are away at meetings and over lunch beaks etc. this risk can be reduced.

Clear screen

All Kingsridge Cleddans Housing Association staff are expected to log off from their PCs/ laptops when left for long periods and overnight. When leaving their desk for lunch or to attend a meeting, users should lock down their screen.

Mobile devices through which access to the network can be obtained, for example PDAs, should be PIN protected, set to power off after a period of 2 minutes and switched off when left unattended. These devices should be stored securely when not in use.

Kingsridge Cleddans Housing Association staff should make sure that open documents on their computer screens are not visible to colleagues or visitors and/or members of the public who are not authorised to see them.

Reporting a security breach

If you suspect that a security breach has or may occur, you must report it immediately.

What to do if you wish to complain about our approach to data security

If any party involved wishes to complain about our approach to Data Security, they should refer to the Director **Error! Bookmark not defined.**who is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines.

Monitoring and Reporting

Regular monitoring and audits will be undertaken by the Data Protection Lead and/or DPO to check compliance with the law, this policy, and associated procedures.

Equality & Diversity

As a service provider and employer, we recognise the requirements of the Equality Act 2010, oppose any form of discrimination, and will treat all customers, internal and external, with dignity and respect. We recognise diversity and will ensure that all our actions ensure accessibility and reduce barriers to employment and the services we provide.