Trafalgar
HOUSING ASSOCIATION

Name of Policy	**Information Security Policy**
Responsible Officer	**Housing Manager**
Date approved by the Management Committee	**27th July 2022**
Date of next Review	**July 2024**

We can produce information, on request, in large print, Braille, tape and on disc. It is also available in other languages. If you need information in any of these formats, please contact us on 0141 952 4676.

TRAFALGAR HOUSING ASSOCIATION

INFORMATION SECURITY POLICY

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, spoken in conversation. It may include personal information about a living individual, or it may be required for the running of **Trafalgar Housing Association**'s business. **Trafalgar 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 **Trafalgar 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 staff 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

This policy will be kept up to date and the latest version will be available for staff to view via the intranet or on request from the Housing Manager.

RESPONSBILITY FOR DATA SECURITY

This policy applies to all employees, directors, consultants, contractors, temporary staff and volunteers.

Each individual has a responsibility to apply adequate security to personal data which it handles to prevent it from being unlawfully accessed, lost, wrongfully deleted or damaged and to comply with this policy. The Director of **Trafalgar 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 which relates to a living individual who can be identified either from that information alone or when that information is combined with other information in our control.

SECURITY MEASURES

We are committed to protecting the integrity of the information we hold. A data security breach could have a very serious legal, financial and reputational impact for us.

TRAINING

Appropriate training will be made available for existing users who have responsibility for information governance duties. Each new employee will be made aware of their obligations for information governance 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 users are adequately trained.

COMPLIANCE AND DISCIPLINARY MATTERS

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.

EQUAL OPPORTUNITES

We are committed to ensuring equal opportunities and fair treatment for all people in relation to our work. In implementing this policy, our commitment to equal opportunities and fairness will apply, irrespective of factors such as gender or marital status, race, religion, colour, disability, age, sexual orientation, language or social origin, or other personal attributes.

Information security procedures:

All staff must adhere to the following procedures to ensure security of **Trafalgar Housing Association**’s personal data:

USE OF HARDWARE & SYSTEMS

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

(a) Using a strong password
(b) Never sharing passwords
(c) Never sharing devices
(d) Locking screens and mobile devices when not in use and ensuring they are physically secure
(e) Ensuring anti-virus is kept up to date
(f) Not downloading unauthorised software or applications onto any of our hardware
(g) Not connecting unauthorised devices or equipment (including USB sticks, printers etc…) to our devices or systems
(h) Not connecting to our systems over unsecured wi-fi

USE OF YOUR OWN DEVICES FOR BUSINESS PURPOSES

You may not use your own personally-owned device for accessing our business information or undertaking work for Trafalgar Housing Association

E-MAILS

You should be diligent when using email to ensure that you do not provide unauthorised access to our information, spread viruses or infect our systems with malware.

- Do not click on hyperlinks or open attachments in emails unless you trust the sender

- Encrypt any documents containing special categories of personal data before sending by email

- Double check the recipients before hitting “Send”

Your company email account remains our property and we may monitor it from time to time to ensure compliance with this policy (subject to any local legal restrictions).

PRINTING

Care must be taken when printing including:

- Only print documents for which you 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 must be shredded

STORAGE OF HARD COPY DOCUMENTS

Any hard copy 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 your documents (eg, over your shoulder when on public transport) – if in doubt do not read such documents in public. If you are using a laptop in a public area you must use a privacy screen to reduce the chance of someone being able to read the contents of your screen.

CLEAR DESK

All users are to leave their desk/workstation paper free at the end of the day.

All users 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.

All office managers should have spare keys for all desks/workstations so that documents can be accessed if the staff member is absent from work.

Users 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 users 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.

All users are to leave their desk/workstation paper free at the end of the day and failure to comply with this instruction, could result in disciplinary action being taken.

CLEAR SCREEN

All users 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 using Ctrl, Alt, Del and then selecting Lock Workstation. The association does have an automatic lock out after an agreed period.

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.

Users 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 to The Director or Housing Manager.

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 who is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines.

REVIEW CYCLE

This document was approved on 27th July 2022 and will be reviewed in 27th July 2024.