Hanover (Scotland) Housing Association

Data Classification Policy

Version: 1.2

Published October 2019

CONTENTS

Document Control

File Name	Data Classification Policy
Original Author(s)	Anup Patel

Version	Date	Author(s)	Notes on Revision
1.0	10 May 2018	Anup Patel	Initial version
1.1	5 July 2018	Anup Patel	Updated
1.2	October 2019	Susan Campbell	Reviewed

Review

This policy shall be reviewed annually by the Director of Organisation Services and amended as appropriate to reflect any changes to the requirements for the use of Hanover (Scotland) Housing Association's information assets. Amendments to the policy will be approved by the Chief Officers. The following table provides a record of these reviews:

Date	Reviewer	Approver	Actions
October 2019	Susan Campbell	Adam Curry	Reviewed

Distribution List

Name	Comment
All staff	Distribute to staff via SharePoint HUB
Interested parties, such as suppliers	Provided as required

1 SCOPE

This document describes the process for classifying information assets within Hanover (Scotland) Housing Association. All Hanover information assets and services are classified taking into account their value, sensitivity and criticality to Hanover as well as any legal obligations relating to contracts.

2 RESPONSIBILITY

All employees and contractors share the responsibility for ensuring that information assets are assigned an appropriate level of protection by following this classification policy.

All owners of information assets are responsible for ensuring that their assets are only accessible to employees of Hanover with appropriate privileges, or to third parties in accordance with this document and where applicable current signed confidentiality agreements are in place.

3 PROCEDURE

3.1 CLASSIFICATION

Hanover classifies information into three levels: Confidential, Internal and Public.

Where indicated below, for documents generated by Hanover the classification information must be included in the document footer, which must be manually set to appear on all pages of the document, or on the media on which it is recorded.

Information received from outside the organisation is re-classified by its recipient so that, within the organisation, it is handled and stored in accordance with this classification. This classification is not necessarily marked on every item but must at least be attached to the container of information so that its classification can easily be determined.

Information sent and received internally that is not marked with a classification level is treated as Internal. Information that is sent externally must be marked with its classification level; any unmarked information sent externally is classified as Public information. If any Internal or Confidential information is sent externally without the correct classification marking, then that action is classed as breaching the company regulations and may be considered misconduct.

The classification of information assets must be reviewed at least once a year by their owners, who determine if the classification level is to be changed.

3.1.1 CONFIDENTIAL

This classification level is for information that has a specific intended internal audience, based on a defined need to know, according to job role.

Confidential information is permitted to be accessed by third parties whose contracts with Hanover authorise access to such information.

Inappropriate disclosure of Confidential information could cause damage, embarrassment and legal repercussions to Hanover, its staff, tenants, or suppliers.

Confidential information sent by email must only be sent to the email address of the intended recipient and may not be copied to individuals or roles that are not authorised to receive it.

Confidential information can only be sent by fax if the nominated recipient is available to receive it directly from the fax machine. Printed copies of Confidential information should be collected from printers without undue delay and should not be left unattended at any time to prevent unauthorised viewing.

Confidential information should be stored on authorised Hanover storage systems, with appropriate permissions set so that only those authorised may access it. Removable and storage media (CD-ROMS, USB sticks, tapes, etc.) may not be used for the storage of Confidential information unless the media is encrypted, or the information itself is encrypted.

Owners of Confidential information should regularly review the distribution to ensure that only the correct people have access.

Examples:

- **Internal documents that are intended strictly for the use of certain internal users** - systems administration guides, network diagrams, certain third party contracts
- **Documents containing personal information** - staff appraisals, personnel records, expense reports, individual salary letters, payslips

- **Tenant data that is only for use by internal staff with a need to know for tenant contracts, sales or relationship management** - tenant details including health data and Next of Kin details, tenant contracts, certain tenant reports

3.1.2 INTERNAL

Everyone on a permanent employment contract with Hanover is authorised to access information with this classification, as are third party contractors whose contracts with the organisation authorise such access and have a need to know.

This information has no restrictions in terms of how it is communicated, other than that it is not cleared for release outside the organisation or to those individuals and/or organisations who sub-contract with the organisation other than where it is has been specifically authorised in advance and contractually documented with that third party.

This information is intended for internal disclosure only and would cause minor damage or embarrassment to Hanover if disclosed externally.

Examples:

- **Internal company information** – Business Continuity Plan, routine reports, monthly reports, Hanover policies, company procedures, proposals, general HR forms, training materials, internal telephone directory

3.1.3 PUBLIC

This is information which can be released outside the organisation and includes documents or information intended for public disclosure.

Examples:

- **Information widely available in the public domain** - public facing website pages, marketing materials, development documents including drawings and building warrants.

3.2 LABELLING

Electronic documents produced by Hanover are labelled as set out above, unless required differently through contract or if requested by a tenant, with the classification set out in the document footer. Documents that do not have footers are marked in alternative appropriate ways. Unmarked documents are automatically treated as Public documents, so care must be taken to ensure that Confidential or Internal documents are not left unmarked.

3.3 CONFIDENTIALITY AGREEMENTS

Hanover makes use of confidentiality agreements, which require the maintenance of confidentiality. These confidentiality agreements fall into the following classes:

- Confidentiality associated with contracts of employment
- Confidentiality agreements issued by Hanover for agreement with tenants or third parties (this should extend to contractual documentation including terms and conditions)
- Confidentiality agreements issued by third parties that Hanover agrees to sign

All of these agreements will in some way cover and obligate Hanover, Hanover employees and other signatories to these agreements to preserving the confidentiality of information exchanged between the parties. Depending on the circumstances that give rise to the need for the agreements, they will typically cover the following:

- Define the information to be protected, its ownership and its classification
- The expected duration of the agreement
- The required actions on termination of the agreement
- Identify the various responsibilities and actions required of signatories in order to avoid unauthorised information disclosure
- Identify the permitted use of the information, and the signatories' rights in respect of that information
- Clarify rights to audit and monitor use of that information

- Describe the process for notification and reporting of unauthorised disclosure or breaches of confidentiality
- Set out the terms for the information to be returned or destroyed at agreement cessation
- Describe the actions that are to be taken if the agreement is breached

Third parties are required to sign a non-disclosure agreement (NDA) prior to being given access to Confidential information. At the discretion of the Director of Organisational Services, third parties may be required to sign an NDA prior to being given access to Internal information.

3.4 STORAGE

Media must be stored in an appropriate clean storage environment.

Asset owners must take proper care in handling data media, as these can be sensitive.

All paper media that has been declared Confidential is stored in lockable filing cabinets with owners identified. Printed material classified as Internal should be stored in locked drawers or cupboards when not in use.

Electronic Confidential and Internal reports or files are stored in approved Hanover storage areas with appropriate access restrictions. Where it is required to store Confidential and Internal information on mobile devices (e.g. laptops), these must be suitably encrypted.

3.5 COMMUNICATION & TRANSMISSION

Electronic or paper information classified as Confidential, if there is a requirement for communication, must be done only on a 'need to know' basis only through an appropriately secure mode of communication. Care has to be taken to ensure that in the TO field and CC list, only authorised people have been added while sending emails.

Electronic or Paper information classified as Internal is communicated to any Hanover staff only. Care is taken to ensure that unauthorised recipients (non-Hanover staff) do not gain access to the contents of such information.

Confidential and Internal information must not be discussed in non-secure environments. This includes being aware of who is around when a telephone conversation is taking place.

Guidance:

Hand carrying:

- Hand carrying of information by Hanover staff is acceptable for any classified information
- Confidential and Internal information being hand carried should be within a sealed envelope, carry case or other receptacle that ensures casual observers cannot see the information
- Confidential information that is stored electronically and transported by hand (CD, USB key, laptop, etc.) should always be encrypted on the storage device

Transmission by post:

- Normal Royal Mail-type delivery may be used for Internal information and Confidential information apart from:
    - Confidential tenant information – where the tenant has specified other means of posting

- Confidential tenant information – for reports to tenants that should be sent by recorded delivery

Transmission by email:

- Within the Hanover email system Confidential and Internal information may be sent by email with regards to the recipient's need to know as described above
- Confidential information that comprises tenant data must be appropriately encrypted if sent out of the organisation by email to any recipient; if a tenant explicitly requests this information to be sent unencrypted this is acceptable if this is received in writing from the tenant
- Confidential information relating to tenants should only be transmitted by email out of Hanover to third party contractors whose contracts with the organisation authorise access to the information and have a need to know
- In some cases, tenants may stipulate how Confidential information is sent electronically; this should be complied with unless the tenant specifies an onerous technique in terms of effort or cost to Hanover in which case the Director of Organisational Services should be consulted and involved in discussion with the tenant to reach agreement on an appropriate approach

Transmission by fax:

- Confidential information can only be sent by fax if the nominated recipient is available to receive it directly from the fax machine
- Internal information may be faxed where it has been confirmed with the receiving party that the receiving fax machine is not in publicly accessible areas of the receiving party's organisation

If there is doubt or uncertainty in the appropriate transmission of information, the applicable information asset owner should be consulted.

3.6 DECLASSIFICATION

Upon review of the classification of all information periodically, the level of classification may change. Such decision to change shall be taken by the Director of Organisational Services and the asset owner. Once the level of classification has changed, the method of handling, storage, and communicating must be changed as per the guidelines defined above.

It should be ensured that after the classification of information is changed, if the classification is reduced (e.g., Internal to Public), it is not given the same level of protection as previously, as this could mean spending resources unnecessarily. At the same time information that has its classification increased (e.g., Internal raised to Confidential) should be treated as required for its new level of classification. Also, should a classification of information change, labelling should be updated for all relevant material

3.7 DESTRUCTION

All information is erased or shredded when obsolete and/or the retention period has been exceeded. Confidential and Internal paper documents for destruction are shredded for secure disposal or placed in secure confidential waste bins.

All hard drives, removable media and any similar items should be securely erased prior to disposal or physically destroying.

For accepted methods of destruction, refer to the Retention section of the Data Protection Policy and Procedures.

Annex A GUIDANCE ON NEED TO KNOW

The term “need to know” is used throughout this document. Generally, all Hanover recipients and producers of information should use common sense in making decisions with respect to classifying information and its handling and storage in accordance with this document. The following can be used as a guide, but it is not intended to be exhaustive nor necessarily to be applied absolutely. Where there is uncertainty the relevant information asset owner should be consulted:

All information:

- Chief Officers of Hanover only

Internal Information

- Everyone on a permanent employment contract with Hanover
- Third party contractors whose contracts with the organisation authorise such access and have a need to know; this should be limited to that information required to fulfil the requirements of contracts or services being provided
- Professional advisors (lawyers and accountants of Hanover) generally have a need to know as required to advise on a case by case basis

Confidential

- Professional advisors (lawyers and accountants of Hanover) generally have a need to know as required to advise Hanover on a case by case basis, limited to that information strictly required to be able to properly advise

Confidential (Tenant Information)

- The Chief Officers of Hanover may from time to time impose further restrictions on a case by case basis which should always be complied with
- Hanover employees involved in the Telecare process or delivery of services to tenants

- Hanover administration staff who require to handle this information to fulfil their duties but strictly to the extent necessary to fulfil the duties (e.g., housing managers)

- Other third parties engaged specifically for the delivery of services to a tenant whose access is to the extent necessary to fulfil those service requirements and only for the duration of those requirements (e.g., plumber attending to fix broken sink)

Confidential (Personal Information)

- Only individuals authorised to access information for a specific task and only to the extent and for a duration that is necessary to fulfil that task or in specific job roles that require access to personal information on an ongoing basis

- Third party contractors whose contracts with the organisation that require a need to know (e.g., outsourced HR services, or insurance brokers); this should be limited to that information required to fulfil the requirements of contracts or services being provided

Confidential (Other Internal Information)

- Systems administration guides, network diagrams, and related documents should only be required by the person(s) responsible for the IT administration of Hanover

- Third party contracts – generally only those involved in negotiating the contracts and agreeing rates will require access; knowledge of the existence of the contracts and any deviations from the standard contract will be required by Director of Organisational Services

- Business Continuity Plan – all Hanover staff require access but no access outside the company