53 Ballindalloch Drive, Dennistoun, Glasgow, G31 3DQ
T: 0141 551 8131 F: 0141 550 2060 E: admin@milnbank.org.uk

Milnbank HOUSING ASSOCIATION

DATA PROTECTION POLICY

LS/OCT.2014/REF.P14

1) INTRODUCTION

Milnbank Housing Association (MHA) recognises that the Data Protection Act 1998 is an important piece of legislation to protect the rights of individuals in respect to personal information that is kept about them, whether on computer or in manual systems. The Association also recognises the need to balance the rights of access with rights of privacy and confidentiality.

The Association is registered with the Information Commissioner as a Data controller and endeavours to ensure that practices in the handling of personal information are of a high standard and complies fully with the Act.

2) PRINCIPLES

MHA has adopted and operates procedures in accordance with the principles of the Data Protection Act. Personal data and information held by the Association shall be:

1st - Processed fairly and lawfully obtained
2nd - Only for specified and lawful purposes, and shall not be used for any other purpose
3rd - Adequate, relevant and not excessive in relation to the purpose for which it is obtained or kept.
4th - Accurate and up to date.
5th - Held no longer than is necessary for the purpose.
6th - Processed in accordance with the rights of data subjects under the Data Protection Act.
7th - Kept securely
8th - Personal data should not be transferred to a country or territory outside the EEA.

Association staff who have access to any personal information shall ensure that they follow these principles at all times. Training will be provided on these principles and the Association's procedures for all relevant staff on a regular basis.

3) TERMINOLOGY

Terminology in the Data Protection Act has a particular legal meaning, it is therefore important that staff and committee members are familiar with these in order to ensure compliance. Key terminology used in the Act includes:

- Data Controller – any individual or organisation that controls personal data (i.e. determines the purposes for which and the manner in which personal data is processed).

- Data Subject – a living individual who is the subject of personal data (e.g. tenant, former tenant, employees, suppliers).

- Personal Data – information held on any living individual which on its own or in conjunction with other information held by the Data Controller identifies that individual (includes audio and video). It includes expressions of option or intention, manual or computerised record.

- Sensitive Personal Data – This is data which relates to a living individual who can be identified and includes personal data relating to an individual's race or ethnic origin, political opinions, religious beliefs, physical or mental health, trade union membership, sexual life, criminal or alleged criminal activity.

- Relevant Filing System – Any set of information relating to individuals and structured, either by reference to the individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible. (E.g. housing files, personnel records, index box files).

- Processing – obtaining, recording or holding data or carrying out any operation on data, including disclosure and destroying information.

4) RESPONSIBILITIES FOR COMPLIANCE

It is essential that the Association does not obtain, process and store information for any purpose other than those they have registered for. In order to comply with the Act, staff must be aware that this relates to information held on residents and former residents, applicants for housing, applications for employment, employees, pension administration, committee members and supplier administration. For clarification purposes, the undernoted defines the responsibilities for data protection within the Association.

a) The Directorate has overall responsibility for data protection within the Association, and for ensuring that notification to the Information Commissioner, and entry in the Data Protection register is accurate and up to date.

b) The Depute Director is the registered Data Controller and will assist in implementing the requirements of the Act by:
   - Providing advice and support to staff on all matters relating to compliance with the Act.
   - Disseminating information relating to the Act.
   - Responding to requests from individuals to access personal information the Association holds about them.

c) The Depute Director has specific responsibility for personal information held on employees. Staff will be informed about data protection issues, and their rights to access their own personal data through the staff handbook and induction courses.

d) Functional Line managers will ensure that personal data processed by their function is included in the Association's data protection register is kept up to date and complies with the above principles.

e) All staff have a responsibility to fully comply with the requirements of the Data Protection Act and this policy. When involved in requesting information, staff will explain why the information is necessary, what it is to be used for, and who will have access to it.

5) DATA PROTECTION AUDITS

To ensure compliance all information shall be audited on an annual basis. This will include such information as: residents files, staff records, finance records, shareholders records, committee members records, contractors and suppliers and archived information etc. This will be a systematic process and involve all members of staff Appendix A highlights how this will be implemented.

6) OBTAINING AND KEEPING INFORMATON

The first 5 principles of the Act mean that the Association must establish general standards on how information is obtained, its relevance, accuracy and how long it is kept for. The Act requires information to be adequate, relevant and not excessive.

Access to all computerised data is via a password controlled system whereby all employees are issued with a confidential password. The use of passwords is monitored and changed where deemed relevant.

The general measure that the Association operates to is to ask, "Do we need to keep this information"? then only ask for and retain relevant data. Staff are issued with guidelines to assist understanding of the above statement. Appendix B provides examples of retention periods covering a range of information.

7) ACCESS RIGHTS

Residents, employees and other individuals about whom the Association holds personal information for will have the right to request access to the information, unless it is exempt under the Data Protection Act.

The Association will respond to information on subject access requests promptly and no longer than 20 working days. No charge will normally be made for requests for information. However, the Association reserves the right to make a charge of up to £5.00 to cover administration, stationery and postage costs, where it is felt necessary to do so.

8) CONFIDENTIALITY

Only information which can or must be legally disclosed under the Data Protection Act will be shared with a third party without the individual's consent. Appropriate measures are implemented to ensure security of data.

Confidentiality also extends to employees using all forms of electronic communication. An example of this being social networking whereby Association employees are prohibited from publicly identifying themselves as working for MHA, make reference to the Association or provide information from which others can ascertain the name of the Association.

9) INTERNAL PROCEDURES

In order to assist staff meet the requirements of the Act, an internal Data Protection Procedures manual is available for staff reference.

The Association also operates separate policies for Health and Safety, IT & Acceptable Use and Openness and Confidentiality, all of which relates to the contents of the Data Protection Act.

10) DATA PROTECTION ACT RELATIONSHIP WITH OTHER LEGLISATION

a) Freedom of Information Act 2000
This Act states that Housing Association's, like Milnbank, do not have a statutory obligation to respond to requests for information. The Act does however apply to the Scottish Housing Regulator in that it makes provision for rights of access to information held by the Scottish public authorities, exemptions from the duty to disclose information and the arrangements for enforcement and appeal.

Although Housing Associations are not subject to the FOI Act, they should provide information about their impact on the local environment under the Environmental Information Regulations (e.g. how a new housing development would affect local wildlife)

b) Human Rights Act 1998
The Association shall endeavour to meet the requirements of this Act at all times and aims to balance the human rights of individuals against the rights of the community.

c) Openness & Confidentiality Policy
The Association operates an Openness and Confidentiality Policy which covers Milnbank's position in terms of the use and access to information. For further information, reference should be made to this policy.

d) The Criminal Justice (Scotland) Act 2006
This Act introduced a new duty allowing Housing Associations and the police to jointly prepare and publish anti-social behaviour strategies.

e) Housing (Scotland) Act 2010
This Act gives The Scottish Housing Regulator (SHR) powers to obtain information and carry out inquiries. The SHR can make routine requests for information from Housing Associations (e.g. annual accounts, Scottish Social Housing Charter etc) that are necessary for the purposes of inspection.

f) Bribery Act 2010
The Act introduced rigorous anti-corruption regulations that will affect all employers. The Association has anti-corruption procedures to ensure that precautions are in place to tackle bribery in the workplace. Full details are contained within the Prevention of Fraud & Bribery Policy.

11) MONITORING AND CONTROL

The monitoring and control of the Data Protection Policy is under the remit of the Management Committee. This policy shall be monitored via the Corporate Services Functional Plan and reviewed every two years or as otherwise deemed necessary.

APPENDIX A

DATA PROTECTION POLICY – INTERNAL AUDIT

The purpose of the Internal Audit is to carry out a systematic examination to determine whether activities involving the processing of personal data are carried out in accordance with the Association's Policy and Procedures on Data Protection.

Objectives of the Audit

- To ensure that there is a formal data protection system in place.
- To ensure that staff are aware of its existence, understand and use it.
- To ensure the data protection system is implemented and works effectively.

Data Protection Audit

Each member of staff shall be asked to detail all the personal information they store or require, check computers for spreadsheets, data bases, computerised filing etc, as well as manual records.

Each employee should record:

- What personal data is held?
- Who is responsible for managing the information?
- Where is it stored?
- What do you do with it?
- Why do you need it?
- When was it stored/last used
- Is there duplication? Can data be merged?
- Is there justification for keeping current or archived information?
- Are there statutory requirements to retain information?

APPEDIX B

DATA PROTECTION POLICY – DATA RETENTION PERIOD

	Detail of Information Collected or Held	Location	Purpose Collected or Held	Period Retained For	Exchanged with/Passed on to
1)	Employees' personnel records	Individual files in locked cabinets & computerised secure HR System. Personnel computer records for PAYE, tax, NI contributions., SMP etc	Details of employment and next of kin etc. to meet employment legislation requirements	While in employment & thereafter scanned on secure archived HR computer system. 3 years for statutory payment items e.g. SMP, PAYE and employee disciplinary & grievances. These records may be kept for up to 6 years if required. 6 years for redundancy records. 40 years for pension information & Employee Liability Insurance. 3 years for sickness records.	Details supplied for references, inland Revenue, Pension Scheme, DSS, Dept of Employment, Auditors, Communities Scotland, Lawyers, Employee Counselling Service.
2)	Employees Staff Appraisals & training	Individual files in locked cabinets &	To record employee personal learning &	While in employment & thereafter scanned	Details supplied for reference, Management

	and development records	computerised secure HR System	development	on secure archived HR computer system.	Committee and SHR
3)	Employees Sickness Records	Individual personnel files in locked cabinets with restricted access	Details of staff sickness	From commencement of employment & scanned annually on secure archived HR computer system.	Details supplied for references, Inland Revenue, DSS, Dept of Employment, Auditors, HR purposes and Management Committee
4)	Health & Safety Information	Files in locked cabinet & computerised system. Reference Manuals in box file in policy store.	To record health & safety incidents & keep staff informed.	3 years (Accident Book, records & reports). 40 years for Asbestos & records relating to the Control of Substances Hazardous to Health Regulations. Indefinite for other information	Details supplied for reference, Health & Safety Advisors or representatives.
5)	Recruitment details for job vacancies (application forms and ethnic monitoring details) Disclosure (Scotland) Check forms	Computerised secure HR files. Summary details are retained in secure personnel files.	To provide monitoring details for Equal Opportunities Policy. In case of recruitment enquiry. To meet legislation requirements for safer recruitment & working with volunteers.	Retained on secure archived HR computer system. Destroyed upon receipt, A separate note of disclosure ref, date & job post is kept in personnel file.	Used for monitoring for Management Committee, Auditors and SHR, Industrial Tribunal. Meet requirements of Equality Act 2010. Care Inspectorate inspections.
6)	Employee criminal	Sealed envelope in	Statutory obligations	2 years from date of	Used for SHR and

	conviction details	locked cabinet with restricted access.		employment	Auditors
7)	Ex-Employees' personnel records	Scanned on secure archived HR computer system	Reference for future employees, pension companies	Indefinitely.	Other employers, Pensions, Police, Inland Revenue, DSS, Dept of Employment, Auditors, SHR Lawyers
8)	Association Annual Accounts	Filed on pc with restricted access	Statutory obligation	7 years	References, Auditors, SHR, borrowing facilities.
9)	Contractors Invoices	Stored in lever-arch files in locked cabinets for 1 year then scanned	For auditing purposes	3 years	Auditors and SHR
10)	Debtors invoices	Stored in lever-arch files in locked cabinets for 1 year then scanned	For auditing purposes	3 years	Auditors and SHR
11)	Suspended/cancelled housing list application forms	Scanned into shared drive in computer	Details of applications applying to be rehoused by tenants	3 years	Auditors, and SHR and Management Committee
12)	Ethnic monitoring of housing list applications	Included within housing applications' and noted on SDM	To provide statistics for Equal Opportunities Policy and ARC	3 years	Auditors and SHR
13)	Residents personal files	Scanned into SDM	Details relating to tenancy and management arrangements	Files are scanned from the start of tenancy	Details supplied for references, Auditors, SHR and Solicitors
14)	Past residents personal files	Stored in computer archives in shared drive	Details relating to tenancy and management arrangements	Destroyed on death 3 years after termination of tenancy of or change of owner	Details supplied for references, Auditors, SHR and Solicitors

15)	Tenant rent details	In SDM on each individual tenant account. In shared drive on computer.	To record rent payments, arrears and housing benefit arrangements. To produce monthly reports.	While resident	Details used for SHR, Auditors, Solicitors and Management Committee
16)	Anti-Social complaints records	Recorded in SDM Complaints Package	To record reports of alleged anti-social behaviour and record action taken by Association	While resident	Information used for SHR, Solicitors and Management Committee
17)	Telephone contacts, addresses and email addresses of suppliers, contractors and other contacts	Computerised system with restricted access	To be able to contact people	Indefinitely	Any relevant person who asks
18)	Maintenance job repair lines	Computer folders	Details of individual repairs carried out in properties. To produce monthly reports	3 Years	Details used for Management Committee, SHR and Auditors
19)	Right to Buy and Shared Ownership details	RTB box file in PM office in locked cupboard. Sharing Owners stored in PM office in individual files in locked cabinet.	Statutory obligation	Indefinitely	SHR, publicly available document
20)	Owners factoring details	Individual files in PM office in locked cabinets & personal computer records.	To record factoring payment and arrears. To produce monthly reports	While resident	Details used for SHR, Auditors, Solicitors and Management Committee
21)	Committee members names, addresses, date of birth and code of conduct detail	File in secure filing cabinet.	Regulatory requirement	While a committee member	Used for business planning, Auditors and SHR

22)	Benefit to staff and committee members under Housing (Scotland) Act 2010	Payments & Benefits Register in locked cabinet with restricted access.	Statutory requirements	Indefinitely	Publicly available record, Auditors and SHR
23)	Membership details	Computer database with restricted access.	Statutory obligation	Indefinitely	Auditors, SHR, Management Committee and publicly available document
24)	Complaints to Milnbank Housing Association and the Ombudsman	Computerised Complaints Register with restricted access.	To monitor and record complaints	Indefinitely	Ombudsman, Management Committee, SHR, Auditors and Staff
25)	Owners direct debit mandates showing bank details	Located in Prop Mgt office in locked cabinet and copy retained on SDM	To record factoring payments	While resident	Details used for SHR, Auditors, Solicitors and Management Committee
26)	Potential new customers contact details	Located in Pm office in locked cabinet and copy retained on excel	To allow contact throughout process of taking over as property managers	While potential customers	Details used for Board Meeting
27)	S/A - Current Tenants files	Stored in archer leaver folders in locked cupboards	Held to give tenants access to their folders. To give care inspectorate access to current tenants files when carrying out an inspection	Retained for the duration of tenants stay at project	Archived in white envelopes stored in locked filing cabinet and destroyed after 3 years
28)	SA - Ex Tenants Files	Stored in sealed envelopes in locked filing cabinet	Held to enable care inspectorate to have access to ex tenants files. Senior staff may require access to ex tenants files if asked to attend court etc.	Retained for 3 years	Archived in white envelopes stored in locked filing cabinet and destroyed after 3 years using confidential document disposal company
29)	SA - Referrals for	Stored in archer lever	To enable senior staff	Retained for 6 months	If referral leads to

	support services	folder in locked cupboard	to access to arrange information visits for prospective tenants		placement at project referrals are transferred to tenant's individual file. If referral is cancelled it is transferred to cancelled and suspended referral folder
30)	SA - Cancelled and suspended referrals to support services	Stored in archer lever folder in locked cupboard	To enable senior team to access folder for information or if a tenant is re-referred to look at previous referral to ascertain if there has been any significant issues since last referral was submitted	Retained for 6 months	After 6 months all cancelled and suspended referrals are destroyed using confidential document disposal company
31)	SA - Staff Continuous Professional Development Folders	Stored in files in locked cupboard	To enable interim manager, senior team and individual staff members to have access to files on request and for staff supervisions	Retained for the duration of employment	When employment has ended information in folder is passed to HR
32)	SA - Complaints about the service or staff	Stored in folder in locked cupboard	To provide evidence to external agencies and care inspectorate that any complaints have been dealt with in an appropriate manner	Retained to 12 months	After 12 months any paperwork is disposed using confidential document disposal company
33)	CFN -Child Protection chronologies and files	Child protection Folder in locked filing cabinet in Managers office	To Ensure accurate records are maintained to monitor children and ensure	While child attends Service and for 3 years after they leave	Social Work Services, police, Court officials, Nursery Child Protection Coordinator &

			they are protected from harm		Inspectors.
34)	CFN - Children Files containing contact details and medical needs	In Children's suspension files in locked cabinet in managers office	To ensure each child's need are recorded and met. To ensure families can be contacted in emergency.	While child attends Service and thereafter scanned to secure hard drive for 3 years after they leave	Staff at CFN, Inspectors
35)	CFN - Employee support sessions and file notes	In Employee folder in locked cabinet in Managers office	To ensure staff have access to their support records and action plans. To allow Management to monitor performance levels	While employed at CFN & thereafter scanned on secure archived HR computer system.	Details supplied for references, inland Revenue, Police, Pension Scheme, DSS, Dept of Employment, Auditors, Communities Scotland, Lawyers, Employee Counselling Service.
36)	CFN - Complaints to Carbon Footprints Nursery	Complaints Register Contained in Locked Cabinet in Managers Office	To monitor and record complaints and ensure action arising is carried out	Indefinitely	Care Inspectorate, SHR, Management Committee and Auditors