DATA PROTECTION POLICY

OUTCOME

To provide underlying principles and specific procedures regarding the processing and protection of personal data and sensitive personal data contained within MHA's paper and computerised records. It is aimed at ensuring compliance with the Data Protection Act 1998 and our Values.

SCOPE

All members of staff.

Also the following 'data processors': partner organisations: non-executive board members, contractors, contracted service providers, agency staff and volunteers.

VALUES

This Policy has been developed in line with our Values and should be understood and implemented in that context.

THE DATA PROTECTION ACT

The Data Protection Act 1998 ('the DPA') provides a framework that governs the processing of 'personal data', i.e. information that identifies living individuals. 'Processing' includes holding, obtaining, recording, using and disclosing information. The DPA applies to all forms of media, including paper and images. It applies to confidential information that can be found in residents' and tenants' care documentations and personal file.

Data Protection Act covers information which is held in a Relevant Filing System in such a way that information relating to a living individual may be identified with relative ease. It should not be confused with:

- Requests for access to records relating to someone who has died. This is governed by the Access to the Health Records Act 1990 and our procedure is attached at appendix 1.
- General information held by MHA.
- The Freedom of Information Act 2000, which only applies to public bodies.

If there is any doubt the matter should be referred to MHA's Data Protection Officer.

Some of the terms used in the DPA are defined at Appendix 2.

1. DATA PROTECTION PRINCIPLES

The DPA imposes constraints on the processing of personal information in relation to living individuals. It identifies eight data protection principles that set out standards for information handling. MHA will comply with the eight data protection principles, which require that personal data should be:

1. Fairly and lawfully processed
2. Processed for specified purposes
3. Processed in a way that is adequate, relevant and not excessive
4. Accurate and kept up to date
5. Kept no longer than necessary
6. Processed in accordance with people's data protection rights
7. Kept safe and secure
8. Transferred to countries outside the European Economic Area only with adequate protection

This policy assumes MHA's data processing remains within the EU geographical area. The DPA stipulates more stringent conditions if this is not the case and any such instances must be referred to MHA's Data Protection Officer.

2. PRINCIPLE 1 - FAIR AND LAWFUL PROCESSING

2.1 In practice, this principle means that MHA must have legitimate grounds for collecting and using personal data. MHA must be clear and open with individuals about how their information will be used, and must tell individuals where their information will go or how it will be shared.

2.2 MHA will notify individual residents that we will abide by the DPA and process their personal data accordingly. The notification for each grouping is as follows:

- Residents / Live at Home Members - Agreement
- Staff Members - Employment Policies And Procedures Manual
- Volunteers - Induction Pack
- Donors – Website

2.3 MHA will process personal data lawfully, in accordance with at least one of the 'conditions for processing', as set out in Schedule 2 of the DPA. The conditions for processing are set out in full at Appendix 3. In practice, the conditions that are most likely to be satisfied are either:

- the individual has consented to the processing,
- the processing is necessary to protect the vital interests of the resident i.e. in a life or death situation, or
- there is a legal obligation to process the personal data.

2.4 The DPA places more stringent conditions on the processing of 'sensitive personal data'. Sensitive personal data is defined in Appendix 2 of this policy, but it includes information as to:

- The racial or ethnic origin of an individual.
- The physical or mental health or condition.
- The religious beliefs or other beliefs of a similar nature.

MHA will process sensitive personal data in accordance with the DPA. This means that sensitive personal data will only be processed where one of the 'conditions for processing' as set out in Schedule 2 of the DPA is met (see 2.3 above) and where one of the other following conditions is also met:

- The individual has given their explicit consent to the processing.
- The processing is necessary for compliance with employment law.
- The processing is necessary to protect the vital interests of the individual or another person.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings, for obtaining legal advice or for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes and is undertaken by a health professional.
- The processing is necessary for monitoring equality of opportunity and is carried out with appropriate safeguards for the rights of individuals.

2.5 MHA will not send unsolicited direct marketing communications to anyone who has indicated that they do not want it, and will not pass, share or sell personal data to third parties for their marketing purposes.

2.6 MHA's use of Closed Circuit Television (CCTV) is for security and crime detection only. Details are included at appendix 6.

3. PRINCIPLE 2 - PROCESSED FOR SPECIFIED PURPOSES

3.1 MHA will process personal data only for specified purposes. These purposes are disclosed to the Information Commissioner and listed in Appendix 4.

3.2 The Data Protection Officer authorises all personal data processing, submits applications for notification and completes an annual notification renewal to the Information Commissioner.

3.3 If a MHA staff member wishes to initiate a new system which would entail processing new personal data or existing data for a new purpose, then this must be referred to the relevant Director and MHA's Data Protection Officer who will guide MHA staff members, with legal assistance if needed.

4. PRINCIPLE 3 - ADEQUATE, RELEVANT AND NOT EXCESSIVE

4.1 MHA will seek to ensure all personal data processed is adequate for the specified purpose. MHA should not obtain or hold more information than is needed.

5. PRINCIPLE 4 - ACCURATE AND UP TO DATE

5.1 MHA will seek to ensure all personal data processed is accurate initially and updated as necessary.

6. PRINCIPLE 5 - KEPT FOR NO LONGER THAN IS NECESSARY

6.1 MHA will seek to ensure that personal data is not kept for longer than is necessary. Personal data should be updated, archived or securely deleted if it goes out of date.

6.2 MHA will seek to ensure all personal data processed is stored and filed consistently and logically, and that data is retained only for relevant periods.

6.3 Details are attached in Appendix 5 regarding retention periods for the different categories of data.

7. PRINCIPLE 6 - PROCESSED IN ACCORDANCE WITH PEOPLE'S DATA PROTECTION RIGHTS

7.1 The DPA gives rights to individuals in respect of the personal data that organisations hold about them. MHA will ensure that personal data shall be processed in accordance with those rights. MHA will cooperate with individuals seeking to exercise their rights as fully as possible.

7.2 An individual is entitled to:

- A right of access to a copy of the information comprised in the personal data (see further on this below at 9).
- A right to object to processing which is likely to cause the individual damage or distress.
- A right to prevent processing for direct marketing.
- A right to object to decisions being taken by automated means.
- A right (in certain circumstances) to have inaccurate personal data rectified, blocked, erased or destroyed;
- A right to claim compensation for damages caused by a breach of the DPA.

8. PRINCIPLE 7 - INFORMATION IS KEPT SECURE AND SAFE

8.1 MHA will take 'appropriate technical and organisational measures' to prevent the unauthorised or unlawful processing or disclosure of personal data.

The measures we will take to protect against the loss of personal information will include:

- Technical, e.g.
  - Need-to-know access only to paper and electronic files.
  - Password protection.
  - Encryption.
  - Back-ups.
  - Mobile device security.

- Organisational measures, e.g.
  - Premises are secure.
  - Personal data is not left on desk but locked away.
  - Verify telephone caller identity before disclosing personal data.
  - Computers are turned off when not in use.
  - Procedures for mobile and home workers aimed at preventing third party access to information they are processing.
  - Staff leaver procedures.
  - Confidential data destruction.
  - Training.
  - Staff vetting, supervision and management systems.

Responsible directors/managers should consider the implications of this requirement and ensure security measures are appropriate for the types of data they are processing and ensure records are disposed of securely and according to the timings stipulated in Appendix 5. Confidential paper records must be shredded or disposed of using a specialist confidential waste contractor using sealed bags.

9. SUBJECT ACCESS REQUESTS

9.1 The Data Protection Officer must be informed of all Subject Access Requests by being sent a copy of the form.

9.2 Section 7 of the DPA contains the 'subject access right' (SAR). It is most often used by individuals who want to see a copy of the information an organisation holds about them.

9.3 The SAR entitles the individual to make a request to be granted access to, and be provided with a copy of, any personal data that MHA holds about him or her. This includes a right to be provided with information about the purposes for which MHA processes the personal data, the source of the data, and the logic behind any automated decision making processes.

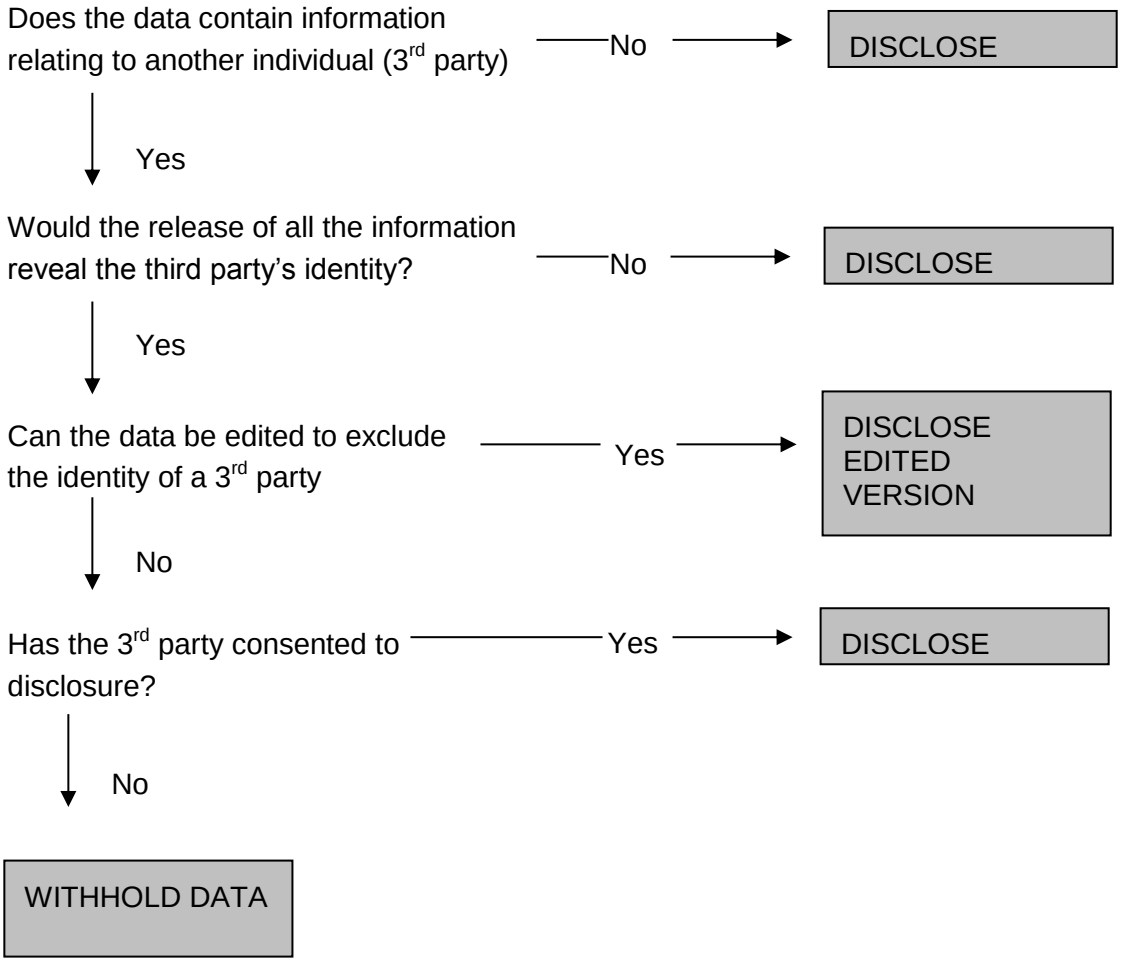
9.4 MHA will not charge a fee for a visual inspection, but may charge £10 for electronic or paper output and up to £50 for medical or educational information.

9.5 SARs must be made using the form found in Appendix 7. On receipt of a completed form we may seek to clarify the exact purpose so that we can target the most relevant data sources efficiently.

9.6 MHA aims to respond to subject access requests promptly and within 40 calendar days of receiving the request form and cleared payment, where required.

9.7 Individuals are only entitled to access their own personal information. MHA should, where necessary, ask the person making the request to provide evidence that they are the individual to whom the personal data relates.

9.8 Before MHA releases any data it must be established whether the identity of a third party might be revealed. If so, please refer to the flow chart below:



9.9 The DPA does not prevent an individual making a SAR via a third party. Often, this will be a solicitor acting on behalf of a resident. In these cases, MHA needs to be satisfied that the third party making the request is entitled to act on behalf of the individual resident, and that the resident has consented to the personal information being disclosed to the third party. It is the third party's responsibility to provide evidence of this entitlement and consent.

9.10 Where a SAR is made on behalf of a resident who does not have capacity to consent to disclosure of their personal information, whether the information should be disclosed or not will depend upon whether the person requesting the information is acting as a representative recognised by law (such as an attorney or deputy) and whether disclosure is in the best interests of the resident. When deciding what is in the resident's best interests, the MDT and statutory consultees will need to be involved in the decision making process, where appropriate.

9.11 If MHA and the individual requesting to see their data fail to agree, the individual may claim compensation, apply to the Court and/or make a request to the Information Commissioner. Any such occurrence should be reported to the Data Protection Officer, who will record this in MHA's Register of Disputed Information Requests.

10. DISCLOSURES TO SOMEONE OTHER THAN THE DATA SUBJECT

10.1 Often a third party, such as a family member, may make a request to see a resident's personal information. MHA will therefore seek to clarify with the resident, before s/he moves in, which individuals should be able to access their personal data.

10.2 From 2013, MHA will record in the Residential Care Agreement (Care Homes) and the Home Care Agreement (Retirement Living) the wishes of the resident in relation to disclosure of personal data. MHA will use to help decide whether or not to disclose personal data to any particular person.

10.3 If a request is made by a third party to see a resident's personal information and the resident has capacity to make decisions about disclosure of their personal information, the residents consent must be obtained before any personal information is disclosed to the third party. As above, any record of prior consent recorded in the Residential Care Agreement/Home Care Agreement will be of use here.

10.4 If a request is made by a third party (including a family member) to see a resident's personal information, and the resident lacks capacity to make decisions about disclosure of their personal information, then whether information should be disclosed to that third party will depend on:

a) whether they are acting as an agent recognised by law, such as a deputy or attorney for the resident; and

b) whether disclosure is in the best interests of the resident.

10.5 There are circumstances under which the Data Subject does not need to be consulted before information is made available, e.g:

- Regulators/commissioners should be given access to information, subject to their acknowledging that we and they have responsibilities under the Data Protection Act, and subject to our being satisfied that it is in relation to their discharging their statutory duties. Copies should be provided at no charge.
- The Police should be given access to personal data on request, subject to our being satisfied that it is in relation to a crime or legal proceedings. Copies should be provided at no charge.

- Health professionals responsible for the clinical care of a resident ie GP, District Nurse or similar, can be granted access to the resident's sensitive personal data subject to our being satisfied that it relates to the mental or physical health of the resident in order to ensure necessary medical care is provided.

10.6 Every third party request to see personal information about a resident should be taken on a case by case basis, and staff members should seek guidance from their senior manager. If the matter is complicated, the matter should be referred to the Data Protection Officer or legal advice should be sought.

10.7 All third party requests to see personal information about an individual resident must be in writing. Proof of identity must also be provided.

11. ACCESS TO HEALTH RECORDS OF DECEASED RESIDENTS

11.1 For guidance on the access to health records of a deceased resident see Appendix 1.

12. DISCLOSURES TO OUTSIDE ORGANISATIONS

12.1 MHA may receive requests for disclosure of residents' personal information from other outside organisations, such as commissioners, adult safeguarding authorities and the police. Disclosure of personal information to these organisations may be permitted in certain circumstances, but decisions about disclosure should be taken on a case by case basis. Contact the Data Protection Officer for advice.

13. DPA BREACHES

13.1 Breach of this policy by any employee is a disciplinary offence, which may result in dismissal. Breach of this policy by any other data processor will constitute a breach of contract with MHA and may result in the termination of the contract.

13.2 If MHA breaches the DPA, the Data Protection Officer must be advised immediately. Appropriate advice on how to manage the breach will be provided to the member of staff and, if necessary, the Data Protection Officer will advise the Information Commissioner of the matter. MHA will manage breaches in accordance with the Information Commissioner's published guidance. Failure to act on the advice of the Data Protection Officer within the agreed timescale may result in disciplinary action being taken.

13.3 Potential breaches include, but are not limited to:

a) Loss/theft of mobile phone or portable storage device
b) Loss/theft of laptop
c) Loss/theft of personal file
d) Providing data to an un-authorised person
e) An un-authorised people accesses confidential files

APPENDIX 1

1. ACCESS TO HEALTH RECORDS RELATING TO SOMEONE WHO HAS DIED

The right to access the health records of a deceased resident is governed by the Access to Health Records Act 1990 ('The AHRA'). This Act provides that an individual is entitled to access the records of a deceased person if:

a) they are the deceased's personal representative (i.e. the executor or administrator of the deceased person's estate), or

b) they have a claim arising out of the resident's death.

Otherwise the documents are subject to confidentiality.

A person who was nominated to be an attorney under a Lasting or Enduring Power of Attorney does not have an automatic right to see the health records of a deceased person, because the power conveyed by the Lasting/Enduring Power of Attorney ceases on at death of the Data Subject.

A personal representative has an unqualified right of access to a deceased person's health record and does not need to give a reason for applying for access to the health records.

Other individuals only have a right of access when they can establish a claim arising out of the resident's death. Determining whether a claim exists lies with MHA. This can sometimes be difficult to determine, and therefore legal advice should be sought if necessary.

2. APPLYING FOR ACCESS

A request for access to health records under the AHRA should be in writing. The request should give details of the applicant's right to access the records. If it does not, MHA should ask the applicant to clarify the basis on which they are applying to see the records.

MHA may need to ask the applicant to provide evidence of their identity and evidence to support their claim, if applicable.

Any such requests should be referred to the Director of Quality who will seek to ascertain whether the individual is entitled to access the records as indicated above.

APPENDIX 2

TERMINOLOGY DEFINED

The following terms are used throughout this Policy and its application. These definitions align with those used within the DPA. Each term is defined as follows:-

1. DATA CONTROLLER

1.1 A 'Data Controller' is the person who determines the purpose, and the manner, in which personal data are processed. For Personal Data which is under MHA's control this is MHA together with those within MHA who take the decisions about how and why personal information is to be processed.

1.2 In some cases MHA receives Personal Data from another person, and we process it for their purposes and under their instruction. In such cases the other person is the Data Controller.

2. DATA PROCESSOR

2.1 A 'Data Processor' is a person who processes Personal Data on behalf of the Data Controller and is instructed by the Data Controller, but who is not an employee of the Data Controller. So any person, public authority or other body processing Personal Data on behalf of the Data Controller is a Data Processor. This includes electronic publishing and those who collect information on behalf of others.

2.2 Examples of data processors:

- External researchers providing a service for MHA.
- Independent tenant participation advisors who may have access to some information about other tenants.
- Maintenance contractors who receive tenant contact and appointment details.
- Builders and major works contractors who receive tenant contact and appointment details.
- Managing agents acting for MHA.
- External auditors (professional service providers) who may review customer records in the course of providing their services for MHA.
- Regulators who may review customer records such as in the course of performing inspections.
- Recruitment Agencies acting for MHA.
- External payroll agencies who provide services to MHA.

3. DATA PROTECTION OFFICER

3.1 The '**Data Protection Officer**' is the person nominated by the Chief Executive to take responsibility for corporate compliance:

Andy Godfrey - andy.godfrey@mha.org.uk

4. DATA SUBJECT

4.1 A '**Data Subject**' is any living individual who is the subject of Personal Data.

4.2 There are no age restrictions on who qualifies as a Data Subject but the definition does not extend to individuals who are deceased.

MHA's Data Subjects include: residents, tenants, Live at Home members, donors, volunteers and members of staff.

5. PERSONAL AND SENSITIVE PERSONAL DATA

5.1 Personal Data

Data which relate to a living individual who can be identified:

a) from those data

b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any in indications of the intentions of MHA or any other person in respect of the individual.

Examples of personal data:

- Age
- Marital status
- Housing history of an individual
- Economic status of an individual
- An individual's allowance, benefits and grants
- Support services received by an individual
- Medical data
- Attitudinal data
- Mailing lists

5.2 Sensitive Personal Data

The DPA recognises that some items of data are more sensitive than others, and therefore require additional legal protection to ensure appropriate handling.

Sensitive personal data Includes Information on:

- race or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- membership of a trade union
- physical or mental health or condition
- sexual life
- the commission, or alleged commission, of any offence
- the proceedings for any offence, or alleged offence

6. PROCESSING OF PERSONAL DATA

The definition of '**Processing**' is very wide. Processing means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the Information or data.

Processing can be manual or automated.

7. RECIPIENT

A '**Recipient**' is any person to whom personal data are disclosed, whether or not the disclosure is intentional or lawful.

8. RELEVANT FILING SYSTEM

'a Relevant Filing System' means:

- a set of information, stored electronically or on computer, which is structured, either by reference to individuals or criteria relating to individuals, in such a way that specific information about a particular individual is readily accessible.
- A useful rule of thumb in working out whether a file is likely to be covered is whether a temporary worker, who is not familiar with the filing system, if instructed to find a particular piece of information, would be able to do so easily and in particular without leafing through the whole file.

9. THIRD PARTY

'**Third party**' relates to any person other than the individual (the Data Subject) or MHA.

APPENDIX 3

CONDITION'S FOR PROCESSING PERSONAL DATA

SCHEDULE 2 OF THE DPA

Personal data must be processed in accordance with at least one of the following conditions:

1) The data subject has given consent to the processing.
2) The processing is necessary:
    a) for the performance of a contract to which that data subject is a party, or
    b) for the taking of steps at the request of the data subject with a view to entering into a contract.
3) The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
4) The processing is necessary in order to protect the vital interests of the data subject.
5) The processing Is necessary:
    a) for the administration of justice,
    b) for the exercise of any functions of either House of Parliament,
    c) for the exercise of any functions conferred on any person by or under any enactment,
    d) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
    e) for the exercise of any other functions of a public nature exercised in the public interest by any person.
6)
    a) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
    b) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

APPENDIX 4

DATA PROTECTION REGISTER – ENTRIES

Methodist Homes

Purpose		Dept / Function	Responsibility
1	Accounts and Records	Residents' Income	GFD
2	Advertising Marketing & Public Relations	Supporter database Sales initiatives	GDPCA
3	Staff Administration	HR & Payroll	GDPCA
4	Administration of Membership Records	N/A	N/A
5	Trading / Sharing in Personal Information	N/A	N/A
6	Fundraising	Supporter database	GDPCA
7	Legal Services – Income / Legacies / Power of Attorney	Legal	GFD
8	Realising the Objectives of a Charitable Organisation or Voluntary Body	Legal	GFD
9	Crime Prevention and Prosecution of Offenders	CCTV / Estates	GDCH
10	Health Administration and Services	Care	GDPCA

MHA Auchlochan

Purpose		Dept / Function	Responsibility
1	Staff Administration	HR & Payroll	GDPCA
2	Accounts and Records	Residents' Income	GFD
3	Health Administration and Services	Care	GDPCA
4	Crime Prevention and Prosecution of Offenders	CCTV / Estates	GDCH

Methodist Homes Housing Association

Purpose		Dept / Function	Responsibility
1	Accounts and Records	Residents' Income	GFD
2	Advertising Marketing & Public Relations	Supporter database Sales initiatives	GDPCA
3	Staff Administration	HR & Payroll	GDPCA
4	Administration of Membership Records	N/A	N/A
5	Trading / Sharing in Personal Information	N/A	N/A
6	Fundraising	Supporter database	GDPCA
7	Legal Services – Income / Legacies / Power of Attorney	Legal	GDRL
8	Realising the Objectives of a Charitable Organisation or Voluntary Body	Legal	GDRL
9	Crime Prevention and Prosecution of Offenders	CCTV / Estates	GDCH
10	Health Administration and Services	Care	GDPCA
11	Property Management	Tenancies/Lease hold	GFD

Key:

- GFD Group Finance Director
- GDPCA Group Director People and Corporate Affairs
- GDCH Group Director Care Homes
- GDRL Group Director Retirement Living

APPENDIX 5

MHA'S PERSONAL DATA TYPES AND RETENTION PERIODS

The responsible Director (as indicated below) should liaise with the Data Protection Officer in all matters referred to the Information Commissioner.

Legal advice should be sought by the responsible Director from their usual lawyers. A member of the Leadership Team (LT) should be involved if there is any doubt or complication.

These retention periods apply to paper, electronic (document or database) and email records.

A Residents / Live at Home Members

– Responsibility: Director of Care Homes or Director of Retirement Living

Record	Retention Time
Residents' records – England and Wales	8 Years from date of last entry
Residents' records – Scotland	7 Years from date of last entry
Live at Home members' records – Britain	3 Years from date of last entry

– Responsibility: Director of Finance

Record	Retention Time
Debtors and Creditors finance records (inc. residents and tenants) - Britain	7 Years

B Staff Members

– Responsibility: Director of People Development

Staff Members' Record	Retention Time
Application Forms, CV's and other unsuccessful applicants' details, selection records.	7 months after applicant notified of outcome unless longer period requested by grant funder e.g. Big Lottery Fund
Employment records /details of terms and conditions	10 years after employee has left employment
Appraisal records /objectives / performance reviews or targets agreed	7 months after employee has left employment
Disciplinary and formal Capability records	- 7 years after the employee has left employment - but, is deemed inactive after 6/12 months from date of disciplinary or formal capability hearing (as per Discipline and Capability Policies)
Pay & benefits information (Inland Revenue requirements)	7 years after employee has left employment
Development / training needs and records of completed activities	7 months after employee has left employment

Category of Worker:	Retained By:
All staff employed in Homes	Home Manager in the Home's administrative office
All staff employed in Retirement Living	Scheme Manager in the Scheme's administrative office
Home Managers	Group Director - Care Homes, Head Office
Retirement Living Managers	Group Director – Retirement Living, Head Office
Regional and Head Office staff	Group Director or HR Director – Head Office
Group Directors	Chief Executive – Head Office

C Health & Safety – Responsibility: Director of Quality

Record	Retention Time
All Health & Safety records except asbestos records	8 Years
Asbestos records	40 Years

D Volunteers – Responsibility: Director of People Development

All records pertaining to volunteers should be kept for the same length of time as indicated for staff members in 'B' above.

The records should be retained by the local home or scheme manager in the administrative office.

E Donors / Potential Donors – Responsibility: Director of Chaplaincy

All records to be retained for 8 years after the last communication with MHA.

F CCTV Recordings – Responsibility: Property Director

Record	Retention Time
CCTV recordings	1 month, unless being retained for evidential purposes.

APPENDIX 6

USE OF CCTV

1 CCTV recordings are primarily used for security & crime detection, but can incidentally be used if they reveal activity that no employer can reasonably be expected to ignore.

2 Recordings must record the date and time accurately and the accuracy of the system must be checked every 6 months

3 Cameras must only cover areas deemed necessary

4 CCTV signage should be placed so that the public are aware that they are entering a CCTV area and it should state, 'images are being recorded for the purpose of crime prevention and detection. The scheme is controlled by Methodist Homes Tel: 01332 296 200'.

5 Access to images should be restricted to a manager or designated member of staff who will decide whether to allow requests for access by third parties in accordance with this policy.

6 Live video feed screens should be placed so they are not viewable from public areas.

7 Any media containing recordings must be stored in a secure, lockable location.

8 Access to recordings must be based on a date and time range.

9 Access Requests should be referred to the Estates Manager and should be processed within 40 days

10 Subject Access Requests must specify the date and time range to be searched and must be for security or crime detection purposes.

11 In order to comply with the protection of other people the images or video may need editing before releasing to the Subject. Any third party doing the editing must provide a guarantee of privacy.

APPENDIX 7

METHODIST HOMES

SUBJECT ACCESS REQUEST FORM

To: _____

From: _____ _____
Name Address

_____

Date: _____ _____

_____

I am writing to request that you provide a copy of the following personal data which you may be holding in a filing system such that I may be identified:

I understand that the information will be provided within 40 days of the above date.

Signed: _____ Date: _____

For official use only

Received _____ _____
Name Date

Action: _____

Supplied _____ _____
Name Date