

# **Data Protection Policy and Guidance Notes**

## **HR15**

# Contents

1. Policy statement.....	1
2. Purpose.....	1
3. Scope.....	1
4. Responsibilities .....	1
5. Definitions .....	1
6. The Requirements under the GDPR .....	3
7. Lawfulness and Fairness .....	5
8. Transparency .....	6
9. Purpose Limitation .....	6
10. Data Minimisation .....	6
11. Accuracy.....	7
12. Retention .....	7
13. Security .....	7
14. Reporting a Personal Data Breach .....	7
15. Transfer Limitation.....	8
16. Data Subject Rights and Requests.....	8
17. Sharing Data.....	9
18. Demonstrating Compliance .....	9
19. Direct Marketing .....	10
20. References .....	10
21. Document control .....	10
22. Equality and Diversity .....	11
23. General Data Protection Regulations (GDPR).....	11
24. Appendix Table.....	11
1 Data Protection Guidance .....	12
2 Confidentiality of Applicant’s and Tenant’s Information .....	13
2.1 Definition .....	13
2.2 General Procedural Considerations .....	14
2.3 Information Received .....	14
2.4 Information Requests from 3 <sup>rd</sup> Parties.....	17
2.5 Information Requests from Tenants, Former Tenants and Applicants .....	19
2.6 Information Requests from Third Parties Acting on Behalf of a Tenant, Former Tenant or Applicant .....	20
3. SUBJECT ACCESS REQUEST .....	21
4. GENERAL – MTHA OFFICES AND STAFF .....	25

*Appendix Two – Data Retention Schedule*..... 28  
*Appendix Three – DPIA Template*..... 28

## 1. Policy statement

- 1.1 This policy provides information about the General Data Protection Regulation ((EU) 2016/679) (“GDPR”) with which Merthyr Tydfil Housing Association (MTHA) must comply.

## 2. Purpose

- 2.1 This policy provides a general overview of the legal requirements included under the GDPR and the Data Protection Act 2018. It sets out what we expect from you in general terms when handling personal information, regardless of the format in which it is stored. This includes information about:

- Current or former employees, workers and applicants
- Current or former tenants and applicants
- Users of our on-line services
- People with whom we engage in relation to our campaigning, fundraising or community activities
- Representatives of organisations with whom we have partnerships, or we are collaborating
- Representatives of our contractors and suppliers

## 3. Scope

- 3.1 This policy applies to all employees and Board members, whether they are employed on a temporary, permanent, voluntary, full-time or part-time basis.
- 3.2 This policy relates to all personal data we process regardless of the format in which it is stored or platform on which that data is stored.

## 4. Responsibilities

- 4.1 All employees / Board members and volunteers must read, understand and comply with this policy when handling personal information on our behalf and attend any compulsory training on its requirements. The policy may be supplemented by specific guidance relevant to your role.
- 4.2 Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

## 5. Definitions

- 5.1 The following definitions are used in this policy:

**Controller** means the person or organisation that determines when, why and how to process personal data. We are the Data Controller of all personal data used in our organisation for our own purposes

<b>Data Subject</b>	means a living, identified or identifiable individual about whom we hold personal data
<b>Data Privacy Impact Assessment (DPIA)</b>	means a tool and assessment used to identify and reduce risks of a data processing activity. A DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the processing of personal data
<b>Data Protection Officer</b>	means the person with responsibility for data protection compliance within our organisation. The current person is the Director of Corporate Services
<b>Personal Data</b>	means any information identifying a data subject or information relating to a data subject from which we can identify (directly or indirectly) a data subject whether from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes special category personal data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour
<b>Personal Data Breach</b>	means any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach
<b>Privacy by Design</b>	means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the data protection legislation
<b>Privacy Notice</b>	means a notice setting out information that should be provided to data subjects when we collect information about them
<b>Processing or Process</b>	means any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties
<b>Processors</b>	means any third parties who we use to process personal data on our behalf

**Pseudonymisation or Pseudonymised** means replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure

**Special Category Personal Data** means information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and relating to criminal offences and convictions

## **6. The Requirements under the GDPR**

6.1 The GDPR requires that personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected only for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- accurate and where necessary kept up to date
- not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage

6.2 Personal data must not be transferred to outside the European Economic Area (EEA) without appropriate safeguards being in place.

6.3 We are required to enable data subjects to exercise certain rights in relation to their personal data.

6.4 We must also comply with particular legal requirements when suppliers that carry out services for us have access to personal data and when we are working with organisations and need to share personal data.

6.5 We are responsible for and must be able to demonstrate compliance with the requirements under the GDPR.

6.6 Service Standards

#### 6.6.1 The Association will:

- Comply with the law (e.g. DPA 2018) with respect to the confidentiality of information.
- Comply with Welsh Government requirements as set out both in the Tenant Guarantee and Performance Standards.
- Deem all personal information held as confidential, only to be released in accordance with this Data Protection Procedure.
- Limit access to confidential information on a strictly need to know basis by using passwords and/or limiting access to folders and files.
- Only store personal information that is relevant to the provision of services to the client.
- Store all personal information securely and ensure that only authorised members of staff have access to it.
- Make staff aware of their obligations under data protection legislation and ensure that clients' personal details are only discussed when necessary to undertake duties effectively.
- Provide staff, Board members and Tenants Voice (TV) with regular training on data protection and information security issues.
- Promote a clear desk policy.

#### 6.6.2 Customer Care and Information

The Association will:

- Inform clients of the Association's commitment and obligations under its Privacy Notice.
- Provide clear, concise and simple to understand information through its Privacy Notice :
  - On its website
  - With the initial information pack provided to tenants
  - At tenancy sign up
  - Information booklet
- Provide easily accessible facilities within its offices for interviews to be conducted in private.

#### 6.6.3 Information Received

The Association will:

- Treat all interviews as confidential and offer to conduct them in private.
- Treat all mail received as confidential and pass anything marked "private and confidential" unopened to the addressee or to the Senior Management Team only.

#### 6.6.4 Third Party Information

The Association will:

- Respect the confidentiality of clients' personal circumstances and ensure that reports to the Board and/or Committees are anonymised.
- Pass information to third parties in accordance with the DPA 2018.
- Ensure that other agencies are aware of our Data Protection practices and that information will only be given in accordance with DPA 2018 requirements.

#### 6.6.5 Training:

The Association will:

- Ensure that all staff, Board members and Tenants' Voice are adequately trained in the Association's Data Protection Policy and Procedures and have a working knowledge of the relevant law. This will include training on the GDPR annually.

## 7. Lawfulness and Fairness

7.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

7.2 You may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

7.3 You may only collect, process and share personal data fairly and lawfully and for specified purposes. The law restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

7.4 The lawful bases available when processing non-special category personal data are:

- the data subject has given consent to the processing of their personal data for one or more specific purposes
- the processing is necessary for the performance of a contract between us and the data subject or in order to take steps at the request of the data subject prior to entering into a contract
- the processing is necessary for compliance with a legal obligation to which we are subject
- the processing is necessary in order to protect the vital interests of the data subject or of another natural person

- the processing is necessary for the performance of a task carried out in the public interest
- the processing is necessary for the purposes of legitimate interests we are pursuing or which a third party is pursuing, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

7.5 A range of additional legal requirements apply when processing special category personal data.

## **8. Transparency**

8.1 The law requires us to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.

8.2 Whenever we collect personal data directly from data subjects, we must provide the data subject with all the information required by the GDPR including the identity of the Data Controller, how and why we will process, disclose, protect and retain that personal data. This is done through a Privacy Notice which must be presented when the data subject first provides the personal data.

8.3 When personal data is collected indirectly (for example, from a third party or publicly available source), we must provide the data subject with the Privacy Notice information as soon as possible after collecting/receiving the data. We must also check that the personal data was collected by the third party in accordance with the law and on a legal basis which contemplates our proposed processing of that personal data.

## **9. Purpose Limitation**

9.1 Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

9.2 You cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the data subject of the new purposes and there is a legal basis for doing so.

## **10. Data Minimisation**

10.1 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

- 10.2 You may only collect personal data that you require for your job duties: you should not collect excessive data. You should ensure any personal data collected is adequate and relevant for the intended purposes.

## **11. Accuracy**

- 11.1 Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.
- 11.2 You should ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You should check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to amend inaccurate or out-of-date personal data.

## **12. Retention**

- 12.1 Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. We will maintain retention policies and procedures to ensure personal data is deleted in accordance with this requirement (see the schedule in Appendix 1).

## **13. Security**

- 13.1 Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.
- 13.2 You are responsible for protecting the personal data we hold.
- 13.3 You may only process personal data when required to do so as part of your role. You cannot process personal data for any reason unrelated to your role.
- 13.4 You must ensure that you follow all guidelines issued to you that are designed to protect against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. You must exercise particular care in protecting special category personal data from loss and unauthorised access, use or disclosure.
- 13.5 You may only transfer personal data to third-party service providers who agree to comply with our policies and procedures and who agree to put adequate security measures in place, as requested. As a minimum this will comprise a signed 3<sup>rd</sup> Party Data Processing Agreement which is recorded in the register (see 17.1).

## **14. Reporting a Personal Data Breach**

- 14.1 The law requires Data Controllers to notify any personal data breach to the Information Commissioner's Office (ICO) and, in certain instances, the data subject.

- 14.2 We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the ICO where we are legally required to do so.
- 14.3 If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. There are significant financial penalties that MTHA could be subjected to (up to 10 million euros or 2% of turnover) where there is a failure to report a personal data breach or a delay in making such a report. You should immediately contact the Director of Corporate Services who is MTHA's nominated Data Protection Officer if you know or suspect that a personal data breach has occurred. You should preserve all evidence relating to the potential personal data breach.

## **15. Transfer Limitation**

- 15.1 The law restricts data transfers to countries outside the EEA where they do not have adequate data protection laws. If you need to send personal data outside the EEA, you should contact the Director of Corporate Services for advice.

## **16. Data Subject Rights and Requests**

- 16.1 Data subjects have rights when it comes to how we handle their personal data. These include rights to:
- where processing is based on the legal basis of consent, to withdraw consent to Processing at any time;
  - receive certain information about the Data Controller's processing activities;
  - request access to their personal data that we hold;
  - prevent our use of their personal data for direct marketing purposes;
  - ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
  - restrict processing in specific circumstances;
  - challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
  - be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
  - make a complaint to the supervisory authority; and
  - in limited circumstances, receive or ask for their personal data to be

transferred to a third party in a structured, commonly used and machine readable format.

- 16.2 You must immediately forward any data subject request you receive to the Director of Corporate Services. See *Appendix 2 – Flowchart of Subject Access Request process*.

## **17. Sharing Data**

- 17.1 You may only transfer personal data to third-party service providers who agree to comply with our policies and procedures and who agree to put adequate security measures in place, as requested. We must have a written data processing agreement in place with any such service providers we are using.
- 17.1.1 A register of all Data Processing Agreements will be maintained for all relevant third-parties, such as contractors, consultants, partner agencies and other service providers as necessary.
- 17.2 In addition, although it is not a legal requirement, it is good practice to have a data sharing agreement with any partners with whom we are working that deals with sharing personal data. It is essential that you have a clear legal basis for sharing personal data with such partners and that you transmit the personal data securely.

## **18. Demonstrating Compliance**

- 18.1 The law requires us to keep full and accurate records of all our processing activities. You should ensure that any processing of personal data that you undertake is included in the records by checking with the Director of Corporate Services.
- 18.2 We are required to ensure all people who work for us have undergone adequate training to enable them to comply with data privacy laws.
- 18.3 We are required to implement Privacy by Design measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.
- 18.4 Data controllers must also conduct DPIAs (appendix 3) in respect to high risk processing. If you believe processing that you are carrying out is high risk, please speak to the Director of Corporate Services. It is MTHA's policy that a DPIA must be completed for each policy whether new or being reviewed, or a new project. The GDPR group meets frequently and discusses the DPIA and recommends it for approval by the Director of Corporate Services.
- 18.4.1 Data Protection Impact Assessments (DPIAs) are a tool which can help MTHA to identify the most effective way to comply with its data protection obligations. The concept of a DPIA has been introduced into UK law by Article 35 of the GDPR.

18.4.2 DPIAs are important tools for accountability, as they help us to comply with requirements of the GDPR, but also demonstrate that appropriate measures have been taken to ensure compliance with the law. In other words, a DPIA is a process for building and demonstrating compliance.

18.5 We must also regularly test our systems and processes to assess compliance. You must regularly review all the systems and processes under your control to ensure they comply with this policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

## 19. Direct Marketing

19.1 We are subject to certain rules and privacy laws when sending marketing material to our tenants or the wider public. You must comply with the guidelines on direct marketing. If you are in any doubt about what this involves, please contact the Director of Corporate Services.

## 20. References

Related External Documents	
Reference	
<ul style="list-style-type: none"> <li>• General Data Protection Regulation (GDPR)</li> <li>• Data Protection Act (2018)</li> </ul>	
Related Internal Documents	
Employee Privacy Notice	
Tenant Privacy Notice & Policy	
Data Protection Impact Assessment (DPIA) form	
Data Retention Policy & Schedule	
Equality and Diversity Policy	
IT User Policy	
Social Media Policy	
Code of Conduct	

## 21. Document control

Document Information	
<b>Business Owner:</b>	Director of Corporate Services
<b>Version no:</b>	2
<b>Effective date:</b>	September 2024

**Review date:** September 2027

**Uncontrolled version if printed or emailed.**

If you are viewing this document from your personal drive, via email or as a hard copy, it may not be the latest version. The current version can be found on the Z Drive:\Policies and Procedures

**Document History**

<b>Date</b>	<b>Version no.</b>	<b>Author</b>	<b>Description</b>
28/08/2020	1	Jane Bamber – HR Manager	Triennial review of policy & update in new format
01/07/24	2	Jayne Lewis – Governance Manager	Triennial review of policy

## **22. Equality and Diversity**

- 22.1 MTHA seeks to treat all employees with fairness and respect and similarly, we expect that all employees treat tenants and other members of the Association with respect. We value diversity and will challenge prejudice and discriminatory behaviour. We will not tolerate racist, sexist or homophobic behaviour, or abuse against anyone with protected characteristics.
- 22.2 Within the scope of this policy, we aim to deal fairly and appropriately with everybody, including those whose actions we consider to be unacceptable.
- 22.3 We understand that periods of trouble or distress can impact on how people usually behave and may lead people to act out of character due to stress or upset. We also recognise that a person's actions may be affected by mental health issues, substance misuse or other factors. We will take these issues and other support needs into consideration when implementing this policy.

## **23. General Data Protection Regulations (GDPR)**

- 23.1 Data will be stored in accordance with the Association's Data Retention Policy.

## **24. Appendix Table**

<b>Appendix Number</b>	<b>Appendix Content</b>
1	Data Protection Guidance
2	Data Retention Schedule
3	DPIA Template

## APPENDIX 1

### 1 Data Protection Guidance

- 1.1 The following guidance has been prepared to offer advice to staff on the obligations of the Association in relation to the Data Protection Act 2018. Under the Act, the Association is defined as the **CONTROLLER** and **DATA SUBJECTS** are all individuals on whom the Association holds personal information. Personal information includes emails of which the individual is a subject and opinions and judgements made of which a record has been kept. This includes electronic records and paper-based files.

1.2	Responsibility for Data Protection	Responsible Department
	The Director of Corporate Services is the Data Protection Officer and has ultimate responsibility for all data protection matters within the Association.	Corporate Services
	The Governance Manager will provide day to day support to the Association on data protection matters	Corporate Services
1.3	Personal Data held by the Association	Responsible Department
(i)	Staff requesting information on behalf of the Association will ensure that it is relevant, accurate, the minimum necessary and suitable for the purpose for which it is required.	All
(ii)	Individuals providing personal data to the Association will be provided with the name of the Data Controller, the purpose for which the information is required, how it will be used and the length of time that that information is to be held.	All
(iii)	The Association will inform individuals when it intends to make decisions relating to them which are based on the personal data that they have provided.	All
(iv)	Staff have an individual responsibility to ensure that any personal data they process/hold is kept securely and remains confidential.	All
(v)	The Association will keep all personal information stored in a safe and secure place.	All
(vi)	Personal data will only be processed in compliance with the Data Protection Act 2018 and, as far as possible, only with the consent of the individual concerned.	All
1.4	Access to Personal Data	
(i)	All data subjects will be informed of their right to access personal data held about them.	All
(ii)	A leaflet will be published and issued to all tenants informing them of their rights under the Data Protection Act 2018	All
(iii)	Upon receipt of a written request from the individual the Association will provide access to personal data held in line with the 'Access to Personal Information' as per section 8. All	DCS/GM

	such requests will be processed via the Governance Manager and Director of Corporate Service (DPO)	
<b>1.5</b>	<b>Rights of individuals</b>	
(i)	<p><i>Data Portability:</i> An individual can ask the Association to provide them with the data in a ‘commonly used and machine-readable format’ so that they can transfer that data to another organisation. This would usually be done using a CSV file. This right only applies where the processing is based on consent or a contract or when the processing is automated.</p>	DCS/GM
(ii)	<p><i>Rectification:</i> If an individual becomes aware of a mistake with the processed data, they have the right to have data corrected. Once corrected, we must inform the individual that we have done so. It is important that if the data is held in a number of places on SDM for example, that it is amended in all places.</p>	All
(iii)	<p><i>Right to Erasure:</i> An individual can ask for their data to be erased in certain circumstances. These include when the processing has concluded, or we hold data on them from when they were under 18.</p>	DCS/GM
(iv)	<p><i>Right to Access:</i> An individual has the right to ask to see the information we hold on them. More detail in section 8 on Subject Access Requests.</p>	DCS/GM
(v)	<p><i>Right to Restrict Processing</i> An individual can ask us to stop processing their data; we can still store it if required. This would include the right to opt out of direct marketing (eg newsletters)</p>	DCS/GM
(vi)	<p><i>Right to Object</i> This is similar to the previous right if we can demonstrate why our need to process the information is greater than the individual’s rights we can continue to process the data.</p>	DCS/GM
(vii)	<p><i>Right to be informed</i> We must tell individuals through our Privacy Notice what we are going to use their data for, how long we will keep it, how they can exercise their rights and the contact details for our Data Protection Officer.</p>	DCS/GM

## 2 Confidentiality of Applicant’s and Tenant’s Information

### 2.1 Definition

For the purpose of this procedure, the following information regarding tenants, former tenants and applicants is defined as confidential:

- Name, address and telephone number
- Date of birth
- Details of current/past circumstances, including employment
- Details of involvement with third parties, eg Statutory and Voluntary Agencies
- Financial circumstances
- Health/medical circumstances
- Details of other members of their household/family
- Racial or ethnic origin
- Religious beliefs
- Offences (including alleged offences)

## 2.2 General Procedural Considerations

- Tenants/former tenants/applicants must always be given the opportunity to discuss confidential matters in private.
- Details relating to a particular tenant/former tenant/applicant should not be openly discussed in office reception areas within hearing of members of the public or with staff who do not require access to the information.
- Details relating to a particular tenant/former tenant/applicant should not be openly discussed outside the office with members of the public or with other members of staff when within hearing of the public.
- All information concerning tenants/former tenants/applicants must be held on file (preferably electronic). Any paper-based files must be securely locked in a cabinet when it is not in use and particularly when the office is unattended.
- All details relating to a former tenant/applicant should be kept for the time period specified in the Document Retention Schedule (<Z:\GDPR\Meeting Minutes & Actions\Data Retention Schedule LIVE.xlsx>) before being destroyed.

## 2.3 Information Received

Confidential information regarding tenants and applicants may be received by post, by telephone, by e-mail or in person (orally or in writing).

2.3.1	<b>Confidential Information Received by POST</b>	<b>Responsible Department</b>
(i)	Information received by post NOT marked PRIVATE AND/OR CONFIDENTIAL should be processed in line with office post opening procedures and then distributed to relevant departments.	Rents & Customer Services

	<p>All such information received should be processed and placed on the applicants/tenants file on the document management system as soon as possible. The original should be securely destroyed.</p> <p>Information received by post awaiting processing/further action should be stored safely and not left in a position where it can be viewed by other people.</p>	Housing/ Maintenance
		All
(ii)	If a request is made to a third party to supply written material that is known to be of a sensitive nature, they should be requested to mark the envelope PRIVATE AND/OR CONFIDENTIAL FTAO ... ( <i>name of Officer to whom the information should be sent</i> )	All
(iii)	Information received by post marked PRIVATE AND/OR CONFIDENTIAL can only be opened by the addressee or a member of the Senior Management Team.	Rents & Customer Services
(iv)	The officer in receipt of the postal information must take a reasonable view as to whether it should be placed on applicants/tenants' file.	All
(v)	If it is felt that the information received is <b>highly sensitive</b> (eg medical papers revealing HIV/Aids status) then such information should NOT be placed on applicants/tenants' file. The information should be passed to the Housing Services Manager who will store the information in the confidential folder on the document management system. Access to this folder is restricted to the Chief Executive, Director of Operations, Housing Services Manager, Senior Housing Officer and the Anti-Social Behaviour Officers.	All  HSM
(vi)	APPENDIX 1 should then be completed and put on the applicants/tenants' file so that it is clear that information has been withdrawn and is held elsewhere. Access to the information held on the Housing Management Confidential File will only be given to the Chief Executive, Director of Operations and the officer who received the information. Requests by any other member of staff to review the confidential information <b>must</b> be referred to the Chief Executive who will determine whether or not access is required in order to carry out their duties effectively.	All DO CEO
(vii)	Officers should always remember that all information stored by the Association <b>must</b> be relevant to the provision of services to a tenants, former tenant or applicant. If it is felt that the information received is irrelevant, it should be destroyed without delay.	All
(viii)	Any concerns or queries as to whether the information should be placed on applicants/tenants' file should be referred to the Data Protection Officer (DPO) or Chief Executive.	All

2.3.2	Confidential Information received by TELEPHONE	Responsible Department
(i)	Information of a confidential nature received by phone should be noted, processed and placed on applicants/tenants' file as soon as possible.	All
(ii)	Information received by phone awaiting processing/ further action should be stored safely and not left in a position where it can be viewed by other people.	All
(iii)	Should the caller state that the information is highly confidential and should not be known by anybody else, the officer in receipt of the information must take a reasonable view as to whether it should be placed on the applicants/ tenants' file.	All
(iv)	If it is felt that the information received is highly sensitive and should not be placed on tenant's/applicant's file, the procedure outlined in point 7.3.2 (v) to (vi) should be followed.	All
(v)	Officers should always remember that all information stored by the Association <b>must</b> be relevant to the provision of services to a tenant, former tenant or applicant. If it is felt that the information received is irrelevant, no record should be kept.	All
(vi)	Any concerns or queries as to whether the information should be placed on the applicants/tenants file should be referred to the Chief Executive.	All
2.3.3	Confidential Information received by E-MAIL	Responsible Department
(i)	Information of a confidential nature received by email should be noted or printed, processed and placed on applicants/ tenants file as soon as possible. The e-mail should then be DELETED.	All
(ii)	Information received by e-mail awaiting processing/further action should be stored safely and not left in a position where it can be viewed by other people. The e-mail should not be left open on the screen and should not be forwarded to any other members of staff.	All
(iii)	Should the sender state that the information is highly confidential and should not be known by anybody else, the officer in receipt of the information must take a reasonable view as to whether it should be placed on the applicants/ tenants' file.	All
(iv)	If it is felt that the information received is highly sensitive and should not be placed on tenant's/applicant's file, the procedure outlined in point 7.3.2 (v) to (vi) should be followed.	All
(v)	Officers should always remember that all information stored by the Association <b>must</b> be relevant to the provision of services to a tenant, former tenant or applicant. If it is felt that	All

	the information received is irrelevant, no record should be kept and the email should be deleted immediately.	
<b>2.3.4</b>	<b>Confidential Information Received in PERSON (in writing or verbally)</b>	<b>Responsible Department</b>
(i)	Information in writing – follow the procedure outlined in point 7.3.1 (v) and (vi)	All
(ii)	Information received verbally – the person should be invited to an interview room to discuss the matter in private. Follow the procedure outlined in point 7.3.1 (v) and (vi)	All

## 2.4 Information Requests from 3<sup>rd</sup> Parties

<b>2.4</b>	<b>Information Requests for 3rd Parties</b>	<b>Responsible Department</b>
(i)	<p>The following information can be provided to the third parties specified below <u>without</u> the tenants/former tenants or applicants permission:</p> <p><u>Information that can be provided:</u></p> <ul style="list-style-type: none"> <li>• Confirmation of name and address</li> <li>• Details of terms of tenancy agreement</li> <li>• Confirmation of tenancy commencement/termination dates</li> <li>• Breakdown of rent paid to the Association</li> <li>• Breaches of tenancy agreement</li> <li>• Details of criminal activity</li> </ul> <p><u>Third Parties to which it can be provided:</u></p> <ul style="list-style-type: none"> <li>• Department of Work and Pensions (DWP)</li> <li>• Local Authorities Housing Benefit Department</li> <li>• Local Authorities Housing Departments</li> <li>• Local Authorities Social Services Departments</li> <li>• Local Authorities Council Tax Departments</li> <li>• Police</li> <li>• Other Housing Associations</li> <li>• Utility Company Suppliers (for the purposes of debt collection).</li> </ul> <p>Any other request should be referred to the Director of Corporate Services or Governance Manager.</p>	All
(ii)	<b>Written permission from the tenant/former tenant/ applicant must be obtained <u>before</u> responding to any other requests for information (see point (vi)).</b>	All
(iii)	Before sharing any of the above information, officers should always ask why the information is being requested to ensure that its' provision is necessary for the third party to undertake	All

	<p>its' duties effectively. The identity of the third party should also be confirmed by:</p> <ul style="list-style-type: none"> <li>• Asking for name, status and telephone number and calling back with the requested information (<b>for requests made by phone</b>);</li> <li>• Ensuring that any information to be supplied following a written request is only done so providing the request was made on official headed paper. Officers should only respond to the name, address and telephone number on the headed paper (<b>for requests made in writing</b>).</li> </ul> <p><b><i>Under no circumstances should any information be provided to a third party without first confirming their identity.</i></b></p>	
(iv)	Any information regarding a tenant, former tenant or applicant supplied to a third party by post must be clearly marked "PRIVATE AND CONFIDENTIAL, F.T.A.O .." ( <i>name of person to whom the information should be sent</i> )	All
(v)	Officers should always inform third parties that the information is being provided on the basis that the principles of confidentiality are observed.	All
(vi)	Details of any information passed to a third party should be recorded and placed on the tenants/former tenants/applicants file.	All
(vii)	When <b>any other</b> requests for information are received, officers should inform the third party that the information <b>cannot be provided without first receiving the tenants, former tenants or applicants written permission</b>	All
(viii)	<p>Officers should contact the tenant, former tenant or applicant to obtain written permission to disclose the information (Appendix 2 – spaces on Appendix 2 should be completed <b>before</b> the letter is sent).</p> <p><b>When written permission has been obtained, this should be passed to the Director of Corporate Services or Governance Manager to confirm that the information can be supplied.</b></p> <p>If the tenant, former tenant or applicant does not forward their written permission within <b>10</b> working days a reminder letter should be sent asking for a response within <b>5</b> working days (Appendix 3 – spaces on Appendix 3 should be completed <b>before</b> the letter is sent).</p> <p>If the tenant, former tenant or applicant does not respond to the reminder letter within <b>5</b> working days, officers should contact the third party to inform them that the requested information cannot be supplied because written consent cannot be obtained.</p>	<p>All</p> <p>DCS/GM</p> <p>All</p> <p>All</p>

(ix)	Any queries or concerns regarding the nature of the information being requested or the person making the request should be referred to the Director of Corporate Services or Governance Manager.	All
------	--	-----

## 2.5 Information Requests from Tenants, Former Tenants and Applicants

2.5.1	Information Requests by Phone	Responsible Department
(i)	Confidential information given within an application form for accommodation or during the course of a tenancy <b>must not</b> be discussed on the phone with a caller even if they claim to be the tenant, former tenant or applicant until their identity has been established. This can be done by requesting details of the caller's date of birth, tenant number, application form reference number etc which can be verified against information held on their file.	All
(ii)	Should the tenant/former tenant/applicant fail to provide satisfactory identification they should be invited to write to the Association with their query or to arrange an appointment with a Tenancy Management Officer.	All
2.5.2	Information Request by E-mail	Responsible Department
(i)	Upon receipt of an email request for information, officers <b>must not</b> respond to the email until the sender's identity has been established. This can be done by checking the email address against records held or requesting details of the caller's date of birth, tenant number, application form reference number etc which can be verified against information held on their file.	All
2.5.3	Information Request in Writing	Responsible Department
(i)	Upon receipt of a written request for information, officers should ensure that the hand-writing/signature corresponds with that held on file or that one of the above identification marks, i.e. date of birth, tenant number etc have been provided <b>before</b> supplying the requested information.	All
2.5.4	Information Request in Person	Responsible Department
(i)	Officers should ensure that proof of identity is requested, eg driving licence or that the caller is able to provide suitable alternative identification, eg date of birth, tenant number, application form reference number etc <b>before</b> confidential issues are revealed.	All

(ii)	<b>The only exception to the above requests is where the tenant/former tenant/applicant is known to and recognised by the officer dealing with the enquiry.</b>	All
(iii)	Any queries or concerns regarding the request should be referred to the Director of Corporate Services or Governance Manager.	All

## 2.6 Information Requests from Third Parties Acting on Behalf of a Tenant, Former Tenant or Applicant

2.6.1	Information Requests from Third Parties Acting on Behalf of a Tenant, Former Tenant or Applicant	Responsible Department
(i)	Confidential information given within an application form for accommodation or during the course of a tenancy <b>must not</b> be discussed with any third party claiming to be acting on behalf of the tenant/former tenant/applicant (other than information and third parties covered by point 7.4 (i)).	All
(ii)	When such a request is received either by post, by phone, by e-mail or in person, officers should inform the third party that they are unable to provide the information without first obtaining the tenants, former tenants or applicants written permission.	All
(iii)	To obtain written permission, officers should follow the procedure outlined in points 7.4 (vii) to (ix).	All
(iv)	Where a tenant, former tenant or applicant states that a third party will be acting on their behalf in all future correspondence with the Association, officers should ensure that written confirmation of this arrangement has been obtained prior to supplying any information to the third party.	All
(v)	To obtain written confirmation, officers should forward a 'Confirmation of Communication Arrangements' form (Appendix 4 – officers should insert the name and address of the tenant, former tenant or application on the tear off slip <b>before</b> sending the letter). Other forms of confirmation letter will only be accepted provided that they contain the same information as that contained in Appendix 4.	All
(vi)	Upon receipt of written confirmation, officers should ensure that tenant/former tenant/applicant's handwriting or signature matches that held on file	All
(vii)	All written confirmation should be located in a place that will allow members of staff to see at a glance that special arrangements for communications exist. This might include a diary note/indicator in SDM.	All
(viii)	Upon receipt of a request for confidential information from a third party acting on behalf of a tenant, former tenant or applicant, officers should ensure that the identity of the third party is established <b>before</b> confidential issues are revealed.	All

	<p>This can be done by:</p> <ul style="list-style-type: none"> <li>• Requesting details of the third party's date of birth which can be verified against information held on the 'Confirmation of Communications Arrangements Form' (<b>for requests made by phone, by email, in writing or in person</b>).</li> <li>• Ensuring that the signature corresponds with that held on the 'Confirmation of Communications Arrangements Form' (<b>for requests made in writing or in person</b>)</li> <li>• Viewing third party's driving licence, credit card etc (<b>for requests made in person</b>).</li> </ul>	
(ix)	<b>The only exception to point (viii) is where the third party is known to and recognised by the officer dealing with the enquiry</b>	All
(x)	Any queries or concerns regarding the request should be referred to the Director of Corporate Services or Chief Executive.	All

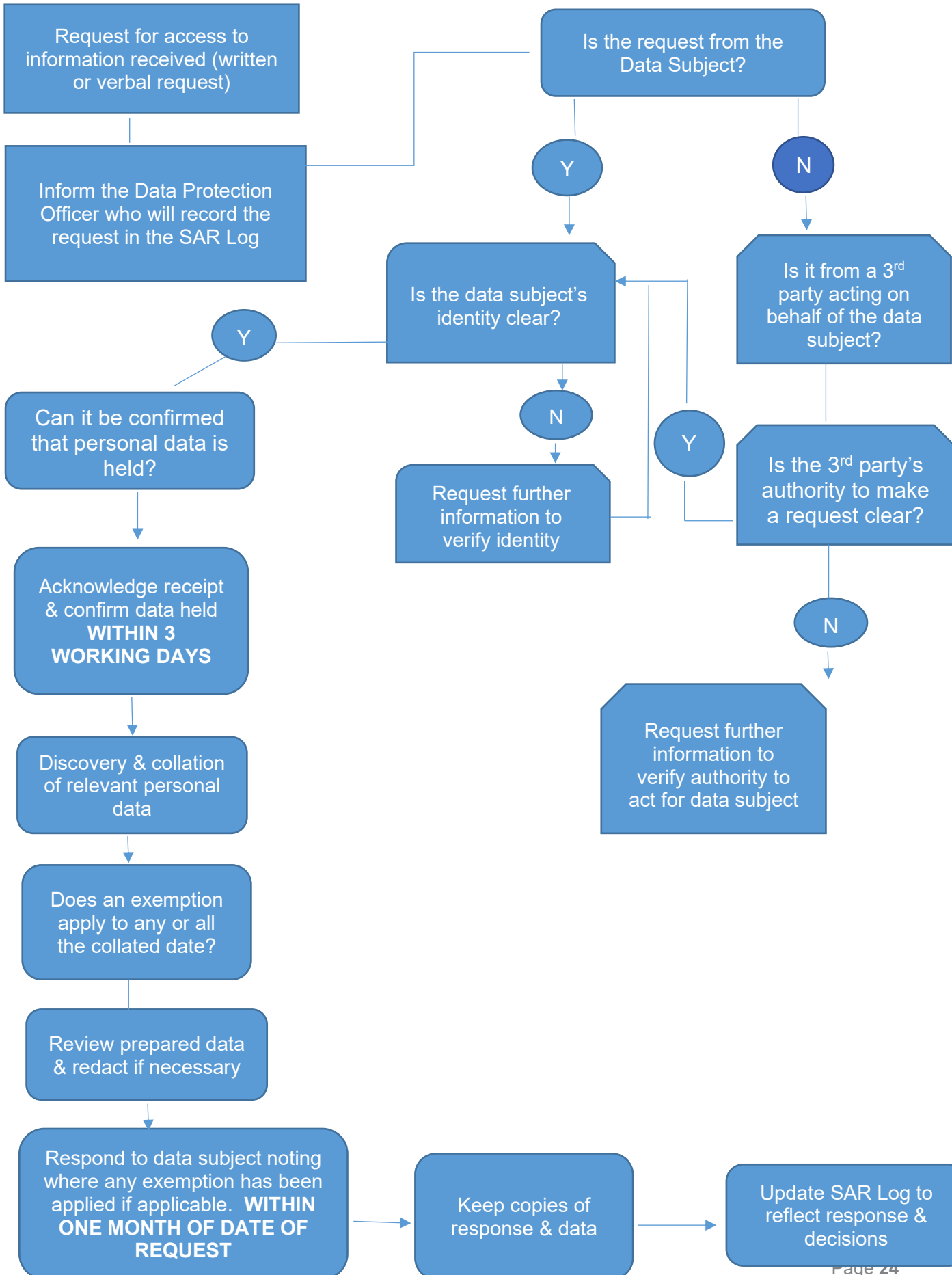
### 3. SUBJECT ACCESS REQUEST

3.1	Subject Access Requests – General Information	Responsible Department
(i)	<p>Any individual whose personal data is held by MTHA has the right to ask to see what records are kept and to request that changes are made if inaccuracies are found. Records may be paper based or held on computer.</p> <p>The request can be made in writing or verbally.</p>	All
(ii)	<p>If the request is excessive or unfounded MTHA is not obliged to answer. There is no standard definition for what this means but the ICO says:</p> <p>“As an example, an organisation may consider a request to be ‘manifestly unfounded or excessive’ when it is clear that:</p> <ul style="list-style-type: none"> <li>• It has been made with no real purpose except to cause harassment or disruption;</li> <li>• The person making the request has no genuine intention of accessing their information (eg they may offer to withdraw their request in return for some kind of benefit, such as payment from the organisation); or</li> <li>• It overlaps with a similar request we are still addressing.</li> </ul> <p>This will be decided on a case-by-case basis, however we must advise the individual within <b>30 calendar days</b> why we have reached that decision.</p>	DCS/GM

(iii)	Any such requests should be as specific as possible. The following are examples of data that individuals may ask to see: <ul style="list-style-type: none"> <li>• Staff <ul style="list-style-type: none"> <li>• HR records including training, appraisals, any disciplinary and grievance processes</li> <li>• Emails of which they are subject</li> <li>• Records held by finance, eg payroll, insurance details, pension details etc.</li> </ul> </li> <li>• Tenants <ul style="list-style-type: none"> <li>• Tenant files</li> <li>• Emails of which they are the subject</li> <li>• Data kept on computer systems (SDM, Invu etc)</li> </ul> </li> </ul>	All
<b>3.2</b>	<b>Procedure for Subject Access Requests</b>	<b>Responsible Department</b>
(i)	The flowchart overleaf shows the process graphically.	
(ii)	<u>Identify the SAR</u> An individual can ask for their data in a variety of ways and it may not always be clear that it is subject access request. We should ask if we are unsure.  The form 'Subject Access Request for Access to Personal Information' (Appendix 5) is available on our website.  We have a calendar month to respond. A calendar month starts on the day the organisation receives the request, even if that day is a weekend or public holiday. It ends on the corresponding calendar date of the next month.	All
(iii)	<u>Acknowledge a SAR has been made and respond to Data Subject</u> Notify the Director of Corporate Services and Governance Manager that a SAR has been received. Send the Acknowledgement Letter (Appendix 6)	All
(iv)	<u>Verify Data Subject's identity</u> As requests can be made via social media or by a member of the general public, we must take every reasonable step to verify the requestor's identity. The search should start during this step.	All
(v)	<u>Request scope of information required</u> If it is unclear what data is being requested, it is acceptable to seek clarification.	All
(vi)	<u>Conduct searches</u> Look through emails, SDM, Invu and paper files for data requested.	All
(vii)	<u>Consider changes to the data during collection and reporting</u>	All

	For certain types of data (eg transactional), the information may change quite frequently. It is ok to update the data as those changes occur. What we cannot do is update or change content because we feel it is embarrassing or inaccurate.	
(viii)	<p><u>Compile and Review</u> Store the data in one secure location and review the material. Look for:</p> <ol style="list-style-type: none"> <li>1. <i>Duplication</i>: have we removed unnecessary copies of the same information?</li> <li>2. <i>Completeness</i>: do we have all the relevant information?</li> <li>3. <i>Exemptions</i>: is there any information covered by an exemption and therefore doesn't have to be disclosed?</li> <li>4. <i>Third Parties</i>: does the material compiled contain information about other people?</li> </ol>	All
(xi)	<p><u>Redaction</u> Information relating to third parties may have to be redacted, especially if they do not agree to their data being shared.</p>	All
(x)	<p><u>Supporting Information</u> We should provide data in clear concise language that the average adult would understand. Our response should include the following information in relation to the personal data that's processed relating to the data subject who submitted the SAR:</p> <ul style="list-style-type: none"> <li>• Types of personal data</li> <li>• Purposes of the processing</li> <li>• Recipients of the personal data</li> <li>• Sources that the personal data is collected from</li> <li>• The retention period for the personal data</li> <li>• Whether the personal data was used for profiling.</li> </ul>	All
(xi)	<p><u>Securely send the information</u> If the data is emailed Egress must be used. If a paper copy is requested, the individual must be given the option to either come to the office to collect it, for it be hand delivered or for it to be sent via Special Delivery.</p>	All

This flowchart describes the steps and decisions made in handling Subject Access Requests from when they are initially received.



<b>3.3</b>	<b>Updating Records to Reflect Inaccuracies or Omissions</b>	<b>Responsible Department</b>
(i)	When an inaccuracy or omission in the personal information held by the Association is discovered by an individual, the following actions should be taken: <ul style="list-style-type: none"> <li>a) For simple changes such as telephone number, these changes should be actioned immediately by the officer.</li> <li>b) For changes to items such as reports, the person should be advised to write to the Director of Corporate Services outlining the reasons for their objection to the report and the action they wish to take.</li> </ul>	ALL
(ii)	The Director of Corporate Services will consider the request and make one of the following decisions: <ul style="list-style-type: none"> <li>• Remove the report from the file</li> <li>• Instruct correction of the particular section of the report</li> <li>• Invite the individual to submit a personal written statement correcting the contents of the report</li> <li>• Decide that the original report is reasonable and accurate and decline the request</li> </ul>	DCS
(iii)	The data subject should be informed of the decision made within seven days. <ul style="list-style-type: none"> <li>• If the decision is to alter the report, a further copy showing the amended details should be provided.</li> <li>• If the decision is to make no alterations, the Director of Corporate Services should explain in a letter why no action was taken.</li> </ul>	DCS
(iv)	Should there be any doubt or concern, the matter should be referred to the Board	DCS/Board
<b>3.4</b>	<b>Complaints</b>	<b>Responsible Department</b>
(i)	Any complaints regarding the operation of this policy should be made through the Association's Complaints Policy and Procedure.	

#### **4. GENERAL – MTHA OFFICES AND STAFF**

<b>4.1</b>	<b>Photographs and Videos</b>	<b>Responsible Department</b>
(i)	If MTHA organises or takes part in public events and we intend to take photographs or videos then we should publicise our intentions (i.e. display written notice). It is not feasible to obtain express permission from all tenants and members of the public.	All

4.2	Recording Telephone Calls	Responsible Department
(i)	Calls received into and out of the main switchboard will be recorded. The telephone system allows for calls to be recorded. This is clearly stated as an automated message for all incoming calls to the Association either through the main switchboard or to a direct line.	All
(ii)	<p>The purpose of recording telephone calls may include:</p> <ul style="list-style-type: none"> <li>• Training and coaching staff</li> <li>• Evidence during misconduct or complaints against staff</li> <li>• Management 'spot check' that customer service standards are being met</li> <li>• Proof of information and advice given to customers</li> <li>• Evidence of abusive calls to staff</li> <li>• There is a threat to the health and safety of staff or visitors</li> <li>• For the prevention or detection of crime</li> <li>• To comply with industry standards and regulatory procedures</li> </ul>	
(iii)	<p>Recordings will be treated confidentially and used, stored and disposed of in accordance with the requirements of the:</p> <ul style="list-style-type: none"> <li>• Data Protection Act 2018</li> <li>• General Data Protection Regulations (GDPR)</li> <li>• The Employment Practices, Data Protection Code</li> <li>• Regulation of Investigatory Powers Act 2000 (RIPA)</li> <li>• The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBP Regulations)</li> <li>• The Telecommunications (Data Protection and Privacy) Regulations 1999</li> <li>• The Human Rights Act 1998</li> </ul>	
(v)	Calls will be stored for 6 months and will be retrievable	
(vi)	All staff will be informed of call recording at induction and regularly reminded.	
(vii)	If and when sensitive personal information is being discussed, it is the responsibility of staff to remind callers that the call is being recorded and to get their explicit consent to continue the call. Any call recording may be subject to a Subject Access Request and claims for professional liability.	
(viii)	Personal information especially special categories personal data, about employees and tenants is shared only with staff who need to know the information in order to carry out their legitimate duties. This may involve sharing information between individuals in different departments.	

(x)	All staff are informed that they are not to write down any payment card details on any paper, book or form when taking payments over the phone. This is part of complying with PCI DSS regulations and is deemed a serious matter if any staff member fails to comply.	
<b>4.3</b>	<b>Staff Responsibilities</b>	<b>Responsible Department</b>
(i)	<p>Details of staff responsibilities in relation to Data Protection will be outlined in the following documents:</p> <ul style="list-style-type: none"> <li>• Contract of employment</li> <li>• Job description</li> <li>• Staff handbook</li> <li>• Staff induction process</li> <li>• Data Protection Policy (FP16)</li> <li>• IT User Policy (FP19)</li> <li>• Home Working Policy, Procedure and Agreement</li> </ul>	All
<b>4.4</b>	<b>Copying Press Articles</b>	<b>Responsible Department</b>
(i)	In order to minimise costs, the Association has chosen not to purchase a copyright licence allowing the unhindered copying of press articles, staff are reminded that photocopies or scans must not be taken of <b>any</b> newspaper or magazine articles. Any articles of interest that a member of staff wishes to retain must be physically cut from the publication concerned.	All

## ***Appendix Two – Data Retention Schedule***

[Z:\GDPR\Policies & Processes \(MTHA\)\New Policies & Processes To be used\Data Retention Schedule LIVE.xlsx](Z:\GDPR\Policies & Processes (MTHA)\New Policies & Processes To be used\Data Retention Schedule LIVE.xlsx)

## ***Appendix Three – DPIA Template***

<..\GDPR\Blank DPIA Template.docx>