TAI CANOLBARTH CYMRU
MID-WALES HOUSING

Yn barod **amdani** **Equal** to the challenge

Gofal a Thrwsio ym Mhowys
Care & Repair in Powys

# Mid-Wales Housing Group Data Protection Policy

| | |
|---|---|
| **Strategic Aim:** | To ensure the Group complies with the requirements of the Data Protection Act 1998. |
| **Reference No:** | Data Protection Policy v1.4 (amended December 2014) |
| **Date Of Issue:** | 24th January 2014 |
| **Next Review Date:** | January 2017 |
| **Departments Affected:** | All Departments |
| **Approved By/Date:** | 22nd January 2014 |
| **Lead Officer:** | Phil Williams, ICT Manager, Mid-Wales Housing Association |
| **Statutory Compliance:** | - Data Protection Act 1998 |

*This page has intentionally been left blank*

**Title:** **DATA PROTECTION POLICY**

## 1. Introduction

1.1 The Data Protection Act 1998 is the latest legislation and covers manual (paper based) records as well as electronic (computer based) records. Individuals therefore have the right of access to any records or information held about them, irrespective of format or storage media.

1.2 Data protection legislation covers (or potentially covers) everyone involved in the Group's business or activities and includes:

- Employees and applicants for employment
- Board and Committee Members
- Tenants and applicants for housing
- Clients and grant recipients
- Contractors, external agents, support providers and consultants

1.3 The Information Commissioner has published the Employment Practices Code. The main part of this document deals with data protection as it relates to employees. While the principles apply, data protection issues relating to tenants, applicants for housing and Care & Repair clients are not specifically covered within the Employment Practices Code.

1.4 This policy covers the Mid-Wales Housing Group. The general principles cover all the activities undertaken by the Group. However, separate sections for the Care & Repair in Powys Agency and Mid-Wales Housing Association are provided where the implementation of the policy is specific to their respective customers.

## 2. Policy Statement

2.1 Mid-Wales Housing Group's policy is to respect the privacy of employees and customers and to comply with data protection legislation. The Group will protect personal data relating to employees and customers and also accepts responsibility for the safe handling of personal data by other people or companies which may be involved in the Group's activities.

2.2 Under the Data Protection Act 1998 there is a duty upon all staff members to be responsible for the way in which personal data is used. The Executive Group of Directors are primarily responsible for the promotion and implementation of data protection legislation within the Group.

2.3 The Director of Finance acts as the Data Protection Compliance Officer for Mid-Wales Housing Association and is responsible for ensuring that all staff fully understand their obligations under the Data Protection Act 1998, that all Directors, Managers and Team Leaders are clear about their responsibilities and that all systems and processes ensure that the legislative requirements are met.

2.4 The Director acts as the Data Protection Compliance Officer for Care and Repair in Powys and is responsible for ensuring that all staff fully understand their obligations under the Data Protection Act 1998, that all Managers and Team Leaders are clear about their responsibilities and that all systems and processes ensure that the legislative requirements are met.

2.5 For clarification of responsibility, the Data Protection Compliance Officer acts as the nominated person within the Association or Agency (an authorised representative of the Data Controller).

## 3. Data Protection Act Principles

3.1 The Data Protection Act 1998 lays down 8 principles regarding the collection, storage and use of personal data:

- It must be obtained and processed fairly and lawfully
- It must only be processed for limited purposes
- It must be adequate, relevant and not excessive
- It must be accurate and kept up to date
- It must not be kept for longer than is necessary
- It must be processed in line with the rights of the data subjects
- It must be kept safe from unauthorised access, accidental loss or destruction
- It must not be transferred to a country outside of the European Economic Area without adequate protection

## 4. Definition Of Terms

4.1 There are various terms used within the Data Protection Act 1998 which are important to understand, as follows:

- "Data"

  This is information that is either processed by electronic (computer) equipment or by a structured (manual) filing system. This includes emails, written correspondence, notes of meetings (referring to an individual) and notes of telephone conversations (about or with an individual).

  Manual records must be "structured in such a way that specific information relating to a particular individual is readily accessible". Therefore, this fully applies to any organised set of papers about an individual.

Personal data is data which relates to a living individual who can be identified from either the data or other information which is in the possession of, or is likely to come into the possession of the data controller. This also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It is important to note that the Data Protection Act 1998 covers only personal data. Therefore general information in the form of statistics or similar formats, from which individuals cannot be readily identified, is not covered by the Data Protection Act 1998.

- "Sensitive Personal Data"

  The Data Protection Act 1998 designates the following categories of information as sensitive personal data:

  - Racial or ethnic origin
  - Political opinions
  - Religious or other beliefs of a similar nature
  - Trade Union membership
  - Physical or mental health or condition
  - Sexual life
  - Offences (including alleged offences)
  - Criminal convictions or proceedings

  Before information on any of the above can be obtained, processed or stored either the individual must give explicit consent or one of a number of conditions must be met. These conditions are:

  - The processing of the data is necessary in order to exercise any right or obligation imposed by law upon the Data Controller (the Group)
  - The processing is necessary within legal proceedings or for establishing, exercising or defending legal rights
  - The information to be processed relates to equal opportunities monitoring
  - The processing is necessary to exercise functions conferred by an enactment of law of statute

  Obtaining a Disclosure on criminal convictions from the Disclosure & Barring Service (formerly the Criminal Records Bureau), collating information on "protected characteristics" to meet the requirements of the Equality Act 2010 would all be covered by one of the above conditions and would therefore not necessarily need the individual's explicit consent under the Data Protection Act 1998.

- "Consent"

  This is the "freely given, specific and informed indication" from the data subject (see below) that signifies agreement to their personal data being processed. This must be in written format (writing, email, text message or fax).

- "Data Processing"

  Obtaining, holding, storing, amending or rearranging personal data or extracting information from it.

- "Data Subject"

  This is an individual who is the subject of personal data, for example, an "employee". A company or organisation cannot be a data subject.

- "Data Controller"

  Mid-Wales Housing Association is registered with the Information Commissioners' Office as the "Data Controller", with a registration number of Z5287937 and is responsible for determining the purposes for which and the manner in which any personal data is processed, or how it is to be processed.

  Care and Repair in Powys is registered separately with the Information Commissioners' Office as the "Data Controller", with a registration number of Z8162536 and is responsible for determining the purposes for which and the manner in which any personal data is processed, or how it is to be processed.

- "Data Processor"

  This is a person other than an employee of the Data Controller who processes data on behalf of the Data Controller. This includes external agents and contractors.

  Where processing is carried out by a data processor, the contract between the Data Controller and data processor must ensure that the data processor is subject to the same obligations regarding data protection as the Data Controller.

- "Notification"

  All companies that hold personal data must notify the "Office of the Information Commissioner" regarding what data is held and also the purpose for holding the data. The notification must cover all possible sources of information and to whom it is intended to disclose the data. A copy of the Data Protection Notification made to the Office of the Information Commissioner is attached as Appendix B.

  The Director of Finance, as Data Protection Compliance Officer for Mid-Wales Housing Association, will review the notification annually to ensure that it covers all personal data that the Association may process.

  The Director, as Data Protection Compliance Officer for Care and Repair in Powys, will review the notification annually to ensure that it covers all personal data that the Agency may process.

- "Recipient"

  In relation to personal data, this is any person to whom the data is disclosed, including any person to whom data is disclosed in the course of processing the data. This does not include any person to whom data is disclosed as part of an

inquiry they have legal power to make (such as a police, customs or trading standards investigation).

- "Third party"

  In relation to personal data, this is any person other than the "data subject", the "data controller" or authorised data processor/person.

## 5. The Employment Practices Code

5.1 The code is not legally binding on employers but represents the Information Commissioner's recommendations as to how employers should fulfil their legal requirements under the Data Protection Act 1998. In the event of a legal challenge against an employer, a Court of Tribunal can take these recommendations into account and evidence of non-compliance be considered. The code has four parts:

- Recruitment and selection
- Employment records
- Monitoring at work
- Information about workers' health

5.2 The code is concerned with information that employers might collect and keep on any individual who might wish to work, currently work or have worked for them. In the code the term "worker" includes:

- Applicants (successful and unsuccessful)
- Former applicants (successful and unsuccessful)
- Employees (current and former)
- Agency staff (current and former)
- Casual staff (current and former)
- Contract staff (current and former)

5.3 Some of the code will also apply to others in the workplace, such as volunteers and those on work experience placements.

## 6. Data Processing

6.1 Throughout employment and for as long a period as is necessary following the termination of employment, Mid-Wales Housing Group will need to keep information about each member of staff for purposes connected with their employment, including recruitment and termination.

6.2 The personal information held will be for management and administrative purposes only.

6.3 The Group has a statutory obligation to provide certain information on employees to its regulatory body, the Welsh Government (and, by virtue of its audit role, the Wales Audit Office) but this is general information in statistical form providing a breakdown of employees by gender and salary bands. The exception to this is the requirement to state the salaries and other benefits of the Officers and Executive Directors.

6.4 There may be other occasions, either now or in the future, on which the Group has a statutory obligation to provide certain information to other bodies. This will normally be in general, statistical format.

6.5 From time to time, the Group compares or benchmarks its performance to the performance of other organisations and information relating to employees may be included. This is in a general format and does not contain personal information relating to an individual employee.

6.6 The Group has a legal obligation to respond to requests from HM Revenue & Customs for specific personal information about individual employees.

6.7 The Human Resources section keeps a personal file on each employee containing the following information:

- Information provided by the employee plus any references obtained during recruitment
- Copy of the Contract of Employment together with any other relevant information about terms and conditions of employment
- Signed job description
- Information about performance including copies of appraisals
- Self-certified sickness absence forms, copies of doctors' statements and correspondence from the employee's doctor or consultant where it has been necessary to obtain this
- Details of any disciplinary investigations and proceedings
- Details of any grievances by or about the employee
- Disclosure & Barring Service (DBS) disclosures and copies of information provided by the employee relating to these
- Training record
- Contact names and addresses
- Correspondence with the Group
- Any other information provided by the employee

6.8 Basic employment details and training records are also kept on a Personnel Database software package, accessible only by authorised users (Chief Executive, Human Resources and ICT staff members).

6.9 The appropriate line manager keeps a personal file on each of their staff members, which may contain the following information:

- Details of terms of employment

- Copy of job description
- Information about performance including copies of appraisals
- Details of any disciplinary investigations and proceedings
- Details of any grievances by or about the employee
- Notes of meetings relating to performance or other issues

6.10 The appropriate line manager also has access to personal employee data for each of their staff members which may contain the following information:

- Home address
- Contact details
- Next of kin
- Date of birth

6.11 The Finance and Human Resources sections keep records and can access electronic information about each employee to enable them to fulfil the company's statutory obligations to HM Revenue & Customs, to pay salaries and to administer the pension and private health schemes. This includes:

- Payroll, tax and national insurance information
- Original doctors' statements
- Details of contributions to the pension scheme
- Details of membership of the private health scheme

6.12 Personal information about each employee is disclosed to external agent "Whittingham Riddell" in order that they can fulfil their role of Payroll and Salary Management. This includes:

- Bank Account details
- Payroll, tax and national insurance information

6.13 Sickness Absence Records

- Self-certified sickness absence forms are seen only by the appropriate line manager (and, for Agency employees, the Finance Officer at Care and Repair in Powys) before being passed to Human Resources to be kept on the personal file.

- Sickness absence records for Mid-Wales Housing Association are stored and managed by the "Vizual Capture IT" database, which is also responsible for building access control, time management (including flexitime). These are accessible only by authorised users (Line Manager, Chief Executive, Human Resources and ICT staff members).

- Sickness absence records for Care and Repair in Powys are stored and managed electronically. The files are accessible only by authorised users (Director, Line Manager and Finance Officer).

- Personal information about actual sickness may be considered and discussed at the appropriate management team meetings only where there is a managerial reason for doing so. In cases of persistent or prolonged absence so that the reasons may be investigated and discussed with the employee.

- Should it be necessary to obtain a report from the employee's doctor or specialist the employee's explicit consent will be sought. A copy of the information thus provided will be made available to the employee if requested.

6.14 References

- References for employees are normally provided by the Chief Executive or the appropriate Director in conjunction with Human Resources (after consultation with the line manager of the employee).

- Before a reference is provided, the employee to whom the reference refers will first be asked if they want the reference to be provided. This also applies if the reference request is unconnected to employment (e.g. mortgage application).

- When an employee leaves they will be asked if they wish references to be provided to future prospective employers.

- An employee does not have the right to see a reference if it is given in confidence for employment purposes by the current employer.

- If an employee asks to see a reference provided by a previous employer or other third party, the Group will only disclose this if it has the consent of the other party or if it is reasonable to comply with the request without this consent.

## 7. Employees' Responsibilities

7.1 To assist the Group in fulfilling its obligations under the Data Protection Act 1998, each employee is responsible for:

- Checking that any information provided to the Group in connection with employment is accurate and up to date

- Informing the Group of any changes to information provided, for example change of address, next of kin, full contact name and contact details.

- Informing the Group of any errors in the information provided, as the Group cannot be held responsible for any errors in data that have not been notified/updated by the employee.

- Ensuring that when dealing with members of the public or external organisations by telephone, email, correspondence or face to face, employees take reasonable steps to confirm the identity of the person requesting information (this would be in

the form of security questions or physical identification such as passport, certificate or copy of household bill). The Group's Confidentiality Policy & Procedures detail the organisations/persons to whom information may or may not be provided.

- Ensuring that all electronic communications comply with the Data Protection Act 1998, as these are also subject to the same regulations as all other forms of communication. The Group's Electronic Communications and IT Security Policy sets out clearly the Group's expectations and requirements upon employees in this regard.

- Protecting personal data and guarding against data security breaches. If it can be shown that employees knowingly misused, recklessly misused or disclosed personal data to a person or organisation for a purpose outside the scope of the Group's notification under the Data Protection Act 1998, then the Information Commissioner has the power to impose fines on both the Group and on the individuals responsible for the breach.

## 8. Directors' Responsibilities

- To fully understand data protection legislation, having primary responsibility for the promotion and implementation of data protection legislation within the Group.

- To ensure that all members of staff under the control of the individual Director are fully aware of their responsibilities regarding data protection.

- To ensure that all data processing is carried out in accordance with this policy document.

- To periodically review personal files (both physical and electronic) and to instigate the review of staff personal files, with a view to updating, removing and/or destroying irrelevant or out of date information.

- Attached to this policy as Appendix A are the "Document Retention Guidelines" for Housing Groups, as supplied by the National Housing Federation. The guidelines contain both statutory and recommended document retention periods. The guidelines are specifically relevant to Mid-Wales Housing Association, but are also helpful for Care and Repair in Powys.

## 9. Security Of Data

9.1 All employees are responsible for ensuring that any personal data that they hold in physical format (e.g. letters, paperwork, point of sale transaction receipts) is kept securely in a lockable filing cabinet, lockable drawer or data safe.

9.2 All employees are responsible for ensuring that all electronic data is kept secure in accordance with the Electronic Communications and IT Security Policy. This also applies to data that is accessed remotely either during homeworking, on laptops or mobile devices (phones and tablets). Data records should not be taken away from the office in an unsecure state (i.e. without being encrypted).

9.3 Under no circumstances should electronic sensitive personal data be transferred or stored on any employee, external agency or third party electronic device (This includes Personal Computers, Laptops, Tablets, Mobile Phones or USB/flash removable memory.

9.4 Sensitive data such that includes unpublished information about the Mid-Wales Housing Group (both Mid-Wales Housing Association and Care & Repair in Powys), including confidential changes to services, performance data, ICT Systems, financial/business planning or other confidential information, must not be divulged to any third party without the express permission of the Director of Finance (who acts as the Data Protection Compliance Officer for Mid-Wales Housing Association) or the Director of Care & Repair in Powys ( who acts as the Data Protection Compliance Officer for Care and Repair in Powys).

9.5 Staff and external agencies that access and/or process employment records, such as personnel, payroll and other related personal information, must pay particular attention to confidentiality and ensure that records are accessed and stored securely.

9.6 All employees are responsible for ensuring that personal information is not disclosed orally (verbally or in writing) or electronically, be it accidentally or otherwise, to any unauthorised third party. Unauthorised disclosure will usually be a disciplinary matter and in some cases may be considered gross misconduct. It may also result in personal legal liability for the individual employee.

## 10. Recruitment And Selection

10.1 The “Application for Employment” form asks only for information which is essential to ensure that the application receives proper consideration.

10.2 A minimal amount of “sensitive personal data” is required on the application form. Where it is required, a sentence will be included on the application form to remind applicants that by providing the sensitive data they are implicitly giving their consent to the Group to use the data.

10.3 Applications for employment are expected to be posted, hand delivered to the Group's offices or completed online on the Group's websites where applicable. Applications sent via email are accepted, although this is not recommended due to the insecure nature of email communications. All applications should be addressed to and/or passed to the Human Resources section, or to the Director of Care and Repair in Powys.

10.4 If, exceptionally, applications are faxed to the organisation, they should be passed immediately to the Human Resources section or Director of Care and Repair in Powys and not left lying on fax machines.

10.5 Some posts will require a disclosure from the Disclosure & Barring Service; in such instances, candidates will be made aware in the application pack that such a disclosure will be required.

10.6 With all applications are included "Equal Opportunities Monitoring" and "How we recruit and select staff" statements that detail the policies and procedures that are followed. The Group aims to ensure that these comply with the principles of the Data Protection legislation. Interview notes are a particularly sensitive area since candidates have the right to see them.

10.7 Completed application forms and interview notes of unsuccessful candidates are retained, securely stored, for 6 months and then destroyed. Recruitment records and interview notes of successful candidates are transferred to their personal file upon commencement of employment.

## 11. Monitoring At Work

11.1 The Employment Practices Code in relation to Monitoring at Work allows employers to undertake various types of monitoring subject to certain conditions and safeguards.

11.2 The Group has the ability to monitor incoming telephone calls for training purposes. This is not an automatic "record all" process but is a manual option. Recordings are stored securely as voicemail messages within the telephone system.

11.3 The Group has a telephone call logging system that monitors traffic both inbound and outbound for tracking purposes, but does not at the present time report on employees' phone usage to make sure that they are not abusing company systems and time. Employees are trusted to make minimal use of the telephone for personal calls.

11.4 Where employees are provided with mobile devices for business use, they are allowed to make and receive personal calls, send and receive personal text messages and utilise data allowances, providing that they do not exceed the monthly contract allowances or impact upon business usage requirements. Where

allowances are breached or business usage impacted as a result of personal usage, employees would be required to identify all personal usage, so that the cost of these can be deducted from their salary.

11.5 The Group does not carry out CCTV surveillance at its offices for security reasons.

11.6 The Group logs and monitors the use of email and Internet access. Full details of this are contained within the Electronic Communications and IT Security Policy.

## 12. Board Members

12.1 Names and private addresses of Board Members are available to staff as well as to statutory bodies such as the Welsh Government and the Financial Conduct Authority. They are not made available to any other body or person. Tenants, clients and members of the public who wish to contact Board Members are requested to send correspondence care of the Association or Agency. Basic information about Board Members is published on the Group's websites (Name, town and brief description of work experience).

12.2 Personal information provided by Board Members during their recruitment or at any time during their period of membership is kept securely by the Chief Executive and the Human Resources section and not divulged to third parties.

12.3 The Group has a statutory obligation to provide certain information about Board Members to the Welsh Government and the Financial Conduct Authority. Other than names and addresses, this is in a generalised, statistical format and does not contain personal information about individual Board Members.

12.4 The amount of personal information held by Board Members about individual employees is limited to:

- Salaries (information required by the Remuneration Committee in relation to the annual salary review, performance pay awards and/or appeals against salary levels)
- Information about disciplinary investigations
- Information about grievances
- Other generalised, statistical data

12.5 Notwithstanding the above, Board Members should follow the principles of data protection outlined within this document.

12.6 Under certain circumstances, Board Members may require a disclosure from the Disclosure & Barring Service; in such instances, they will be made aware that such a disclosure will be required.

12.7 Board Members are also expected to maintain confidentiality about the Group's tenants, clients and activities. A document entitled "Board Member's Guide to Confidentiality" has been issued and should be referred to in this regard.

## 13. Tenants of Mid-Wales Housing Association

13.1 The same data protection principles apply and should be followed in relation to tenants' records as for employees' records. The Association keeps the following tenant information:

- Tenancy Agreement
- Housing Application (including income/expenditure details)
- Equality & Diversity information (Ethnic Origin, Disability, Religion etc)
- Details of special needs or requirements
- Vulnerability indicators
- Special access arrangements
- Contact names, addresses & contact details (telephone, email etc)
- Next of kin details
- Correspondence with the Group
- Detailed tenancy records
- Any other information provided by the tenant

13.2 In particular, tenants' physical information and record files should be kept securely. It is not always practicable to keep these in lockable filing cabinets but, at the very least, they should be filed away at night so that casual visitors to the office cannot gain access to them.

13.3 The majority of tenant personal data records are stored within the Association's Housing Management Database (Capita Open Housing) and within the electronic Association Folder structure. Access is secured and maintained by means of both office access control systems and security passwords. It is vital that these security mechanisms are used appropriately as detailed within the Electronic Communications and IT Security Policy.

13.4 Information about tenants must not be disclosed to unauthorised third parties and references in relation to a tenant's rent record may be only provided with the explicit written consent of the tenant. Further details and guidance can be found within the Group's Confidentiality Policy and Procedures.

13.5 It is a requirement for information to be exchanged between the Association and the Department of Work and Pensions, Housing Benefit Departments, Citizen Advice Bureaux, the County Court and the Police. Protocols should be in place to facilitate such exchange for the benefit of all parties that do not breach the requirements of the Data Protection Act 1998.

13.6 As of 1st January 2015 it is a requirement for Housing Association's in Wales to notify the Water Industry with details of all non-owner occupiers within 21 days of tenancy commencement. The new regulations are called the "Water Industry (Information about Non-Owner Occupiers) (Undertakers Wholly or Mainly in Wales Regulations) 2014". The notification will include a) Property Address; b) Tenancy Start Date; c) Title, Name and Date of Birth for all Adult residents (ages 18 and older). It is also a requirement to notify the residents/occupiers that the information has been provided to the Water Industry.

13.7 Under circumstances where "third party" company schemes (e.g. Home Energy Efficiency Scheme) are available through the Association to its tenants and requests are made by these third parties for personal data. Then specific written consent should be sought from tenants and should be scheme and third party specific.

13.8 Where a tenant is known to be violent or to have other personal difficulties that affect visitors, such information should not be provided to contractors in detail. Contractors should only receive details necessary to complete the assigned task/job (e.g. name/address details) and simply be advised that they should not visit the tenant on their own.

13.9 Where a tenant appears to have mental health problems, the Association is unable to approach another person or body for assistance without the written consent of the tenant. The exception to this would be in emergency where intervention of a third party would be in the best interests of the tenant.

13.10 Specific written consent of the tenant should be sought for pictures taken for publicity purposes. The amount of personal information included in the article or journal should be limited and on no account should the full address or contact details of the tenant be given.

## 14. Clients of Care and Repair in Powys

14.1 The same data protection principles apply and should be followed in relation to clients' records as for employees' records. The Agency keeps the following client information:

- Referral form, including personal contact details and details of alternative contacts (e.g. next of kin)
- Copies of grant/funding application forms and associated paperwork
- Correspondence from third parties relating to work being carried out, e.g. Occupational Health assessments, etc.
- Copies of certificates relating to work carried out on property
- Paperwork relating to property and work being carried out (e.g. Land Registry information, drawings and specifications, etc)
- Copies of financial assessments

- Correspondence with the Agency
- Any other information provided by the client

14.2 In particular, clients' physical information and record files should be kept securely. It is not always practicable to keep these in lockable filing cabinets but, at the very least, they should be filed away at night so that casual visitors to the office cannot gain access to them.

14.3 If, exceptionally, client details are faxed to the organisation, they should be passed immediately to the Director of Care and Repair in Powys and not left lying on fax machines.

14.4 The majority of client personal data records are stored within the Agency's Database (CARIS) and within the electronic Agency Folder structure. Access is secured and maintained by means of both office access control systems and security passwords. It is vital that these security mechanisms are used appropriately as detailed within the Electronic Communications and IT Security Policy

14.5 Information about clients must not be disclosed to unauthorised third parties. Further details and guidance can be found within the Group's Confidentiality Policy and Procedures.

14.6 It is a requirement for information to be exchanged between the Agency and the Department of Work and Pensions, Housing Benefit Departments, Citizen Advice Bureaux, the County Court and the Police. Protocols should be in place to facilitate such exchange for the benefit of all parties that do not breach the requirements of the Data Protection Act 1998.

14.7 Where a client is known to be violent or to have other personal difficulties that affect visitors, such information should not be provided to contractors in detail. Contractors and other data processors (e.g. grant makers) should only receive details necessary to complete the assigned task/job (e.g. name/address details) and simply be advised that they should not visit the client on their own.

14.8 Where a client appears to have mental health problems, the Agency is unable to approach another person or body for assistance without the written consent of the client. The exception to this would be in emergency where intervention of a third party would be in the best interests of the client.

14.9 Specific written consent of the client should be sought for pictures taken for publicity purposes. The amount of personal information included in the article or journal should be limited and on no account should the full address or contact details of the client be given.

## 15. Applicants to the Association For Housing

15.1 The same data protection principles apply and should be followed in relation to applicants' records as for tenants' records. The Association keeps the following tenant information:

- Housing Application (including income/expenditure details)
- Equality & Diversity information (Ethnic Origin, Disability, Religion etc)
- Details of special needs or requirements
- Vulnerability indicators
- Special access arrangements
- Contact names, addresses & contact details (telephone, email etc)
- Next of kin details
- Correspondence with the Association
- Any other information provided by the applicant

15.2 In particular, applicants' physical information and record files should be kept securely. It is not always practicable to keep these in lockable filing cabinets but, at the very least, they should be filed away at night so that casual visitors to the office cannot gain access to them.

15.3 The majority of applicant personal data records are stored within the Association's Housing Management Database (Capita Open Housing), a secure area of the website (where online applications are stored) and within the electronic Association Folder structure. Access is secured and maintained by means of both office access control systems and security passwords. It is vital that these security mechanisms are used appropriately as detailed within the Electronic Communications and IT Security Policy

## 16. Right To Access Information (Subject Access Request)

16.1 Individuals have the right to access personal data that has been kept about them either in organised manual files or electronically and includes opinion and "facts".

16.2 All requests to access or inspect personal data must be made in writing to the Director of Finance who acts as the Data Protection Compliance Officer for Mid-Wales Housing Association, or to the Director of Care and Repair in Powys who acts as the Data Protection Compliance Officer for the Agency. Requests will also be accepted in writing from a third party representative of the individual concerned. However, the Group will take necessary steps to validate the third party representation before granting any requests to access or inspect data.

16.3 Individuals (and third party representatives) requesting to access or inspect personal data will be expected to provide proof of their identity.

16.4 All data supplied will be in a form which the recipient (and/or third party representative) will be able to understand. If the data is coded, then an explanation of the codes will also be supplied.

16.5 The Group will aim to comply with requests for access to personal data as quickly as possible but, in any case, has a statutory obligation to provide the requested information within 40 calendar days.

16.6 The Group is not obliged to disclose the following categories of data:

- If disclosure of the data also involves disclosing data relating to a third party and the third party does not give consent.
- If the disclosure of the data also involves disclosing the intentions of the Group with respect to the requesting individual (e.g. data held relating to the Group's intention to serve a "Notice of Seeking Possession" need not be disclosed).
- If the Group is in receipt of medical opinion that access to the data is likely to cause serious harm or mental health of the requesting individual.
- If the data in question is legally protected
- If the request is for specific data that would be unreasonably difficult to find (e.g. old/archived electronic data or any physical paperwork that is not held in a filing system).
- Any other exemptions under the Data Protection Act 1998.

16.7 The Group is not obliged to disclose the following categories of data to employees:

- Information on disciplinary matters or performance
- Management forecasting and planning if the release of this information would prejudice the business
- Negotiations with the data subject where these could be prejudicial (for example, in cases of redundancy or redeployment)
- Confidential references given by the Group

16.8 The Group may refuse to meet requests for information that are received more frequently than once in three months or twice in any twelve-month period. The Group may also refuse to meet any vexatious requests.

16.9 The Group will make a charge of £10 to fulfil each Subject Access Request.

## 17. Grievances

17.1 If an employee considers that this policy has not been followed in respect of personal data kept about them, the matter should be reported to the Human Resources section. If the matter cannot be resolved it should be raised as a formal grievance under the Group's grievance procedure contained in the Employment Handbook.

17.2 If a tenant, applicant, client or other third party considers that this policy has not been followed in respect of personal data kept about them, the matter should be reported to the Group as a formal complaint using the Complaints Policy & Procedures.

## 18. Document Retention Guidelines

18.1 It is important to periodically review personal data and files (both physical and electronic) with a view to updating, removing and/or destroying irrelevant or out of date information.

18.2 Electronic data and files should be removed or deleted in accordance with the correct procedures of the software, database or electronic storage method used (in accordance with the Manufacturer/Supplier guidelines). All electronic storage media (such as hard drives or data tapes) should be destroyed or securely wiped using "for purpose" software tools or by an approved media/data destruction company.

18.3 Physical data and files should be securely shredded or disposed of by an approved data/record destruction company.

18.4 Attached to this policy as Appendix A are the "Document Retention Guidelines" for Housing Associations, as supplied by the National Housing Federation. The guidelines contain both statutory and recommended document retention periods.

## 19. Related Documentation

19.1 Other policies, procedures and documentation to which reference should be made when considering data protection are as follows:

- Data Protection Act 1998
- Equality Act 2010
- Confidentiality Policy & Procedures
- Board Member's Guide to Confidentiality
- Employment Handbook
- Electronic Communications and IT Security Policy
- Document Retention Guidelines (Appendix A)
- Data Protection Notifications (Appendix B)
- Equal Opportunities Monitoring
- How we recruit and select staff
- Complaints Policy and Procedures

## 20. Review

20.1 The Group's Data Protection policy will be **reviewed every three years** to ensure its on-going relevance.

| | | |
|---|---|---|
| **Strategic Risk Factors** | There are no relevant risks in the Business Significant Risk map, but the following two risk are relevant from the Operational Risk Map<br><br>- Accuracy of Tenant Information (Reference OR11AL001). The risk would be that tenant files and records are not kept up to date and inaccurate information is held about an individual.<br><br>- Security of ICT Systems (Reference OR11IT001). The risk would be that the ICT systems were compromised or policies were not being adhered to, leading to a breach or loss of personal data. | |
| **Equality Impact Audit** | *How does/will this policy ensure needs are met fairly, particularly with regard to race, gender, disability etc?* | Option to include a third-party representative in the Right to Access Information process. |
| | *Is it felt that this Policy might affect different groups adversely. If so what is the justification for this, and is it legally permissible?* | No. This policy serves to protect the rights and personal data of all groups equally and also references the Equality Act 2010. |
| | *Have any representative groups in the locality been asked for their opinion and if so what was the outcome?* | This is not one of the Policy documents on the list for the Equality Review Group to look at. |
| **Tenant Engagement** | *How does/will this policy ensure the needs of tenants are met?* | This policy serves to protect the personal data of tenants and also allow access to view this information upon request. |
| | *How is it felt this Policy will impact on the rights and obligations of tenants?* | This policy upholds the rights of tenants by ensuring that their sensitive personal data is maintained securely and provides a means to access personal data held about them upon request. |
| | *Have tenants been consulted and were the outcomes of that consultation taken into account when considering the* | No. This policy was not amongst those requested to go before T&RF. |

| | | |
|---|---|---|
| | *introduction of this Policy?* | |