Cernach Housing Association
Data Protection and Access to Personal Information Policy & Procedure

1. INTRODUCTION

1.1 The Data Protection Act 1998 (DPA) builds upon the 1994 Act and came into force on 1st March 2000. The prime objective of the Act is to protect the right of privacy of the individual citizen against the misuse of personal data by organisations and restrict the flow of certain information. It gives certain rights to individuals in relation to personal data or information held about them on computer and some manual systems. It requires those who record and use personal information to be open about their use of that information and to develop sound practices. The Data Protection Act contains 8 principles which regulate the way data can be collected, handled and used and these are outlined in section 3 of this Policy.

1.2 In practice all Registered Social Landlords (RSLs) and their tenants and prospective tenants are affected by the Act. All RSLs are subject to the duties under this Act and must register with the Information Commissioner. Notification must include a general description of security measures and include the name and address of the Controller i.e. the Housing Association, description of personal data and data subjects together with the description of the purpose of processing the information and the recipients of that information.

1.3 There are a number of offences, which, if the provisions of the DPA and the Computer Misuse Act are not complied with, will affect the Association and its employees. The general provisions of the Act are:

a) All processing of computer personal data must be registered
b) Personal data must only be processed as specified in the registration
c) Personal data must not be disclosed to any unauthorised person
d) Individuals have, on request, a right to a copy of the data held and appropriate security measures must be taken to protect personal data

1.4 The undernoted are offences under the terms of the Computer Misuse Act

a) Unauthorised access to computer material
b) Unauthorised access with intent to commit or facilitate commission of further offences
c) Unauthorised modification of computer material

1.5 Anyone using another person's user login and password, whether registered or not, will be committing an offence in the first category. The copying of any data not specifically authorised, even into ones own files is an offence in the third category above.

1.6 All staff should note and be aware of their access rights for any given hardware, software or data and should not experiment or attempt to access hardware, software or data for which they have no approval or need to conduct their duties.

2. LEGISLATIVE & REGULATORY FRAMEWORK

2.1 Standard 2 of the Regulatory Standards of Governance and Financial Management states*:"The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these proprieties."* Specifically relating to this Data Protection & Access to Personal Information Policy & Procedure Standard 2.2 states: *"The governing body recognises it is accountable to its tenants, and has a wider public accountability to the taxpayer as a recipient of public funds, and actively manages its accountabilities. It is open about what it does, publishes information about its activities and, wherever possible, agrees to requests for information about the work of the governing body and the RSL."*

2.2 With this in mind, Cernach Housing Association Limited stores personal information both on computer and within manual files and has registered all data processing information with the Information Commissioner. The Association is registered as a Data Controller under the Data Protection Act. (Reg No. Z5533599) and will ensure that our practices in the handling of personal information is of a high standard and complies fully with the Act.

2.3 In accordance with Section 18 of SFHA Raising Standards, the following legislation has also been considered within this Data Protection Policy; Freedom of Information Bill, Human Rights Act 1998, Crime & Disorder Act 1998, Housing (Scotland) Act 2001, Computer Misuse Act 1990, Regulation of Investigatory Powers Act 2000 and Health & Safety at Work Act 1974.

3. PRINCIPLES

3.1 Staff are required to have an understanding and appreciation of the Data Protection Act 1998 in relation to how long to keep data and when the data can be passed on. This legislation protects the information held in manual and computerised records and it applies to: -

- Members of staff
- Members of the Management Committee
- The Association's membership
- Association Tenants
- Former Association Tenants
- Housing List Applicants
- Owners of Properties Factored by the Association
- Sharing Owners

3.2 The Association will adopt and operate procedures in accordance with the Data Protection Act Principles. Personal data and information held by the Association shall:

a) Be obtained and processed fairly and lawfully
b) Be obtained only for specified and lawful purposes, and shall not be used for any other purpose
c) Be adequate, relevant and not excessive in relation to the purpose for which it is obtained or kept
d) Be accurate and up to date
e) Be held no longer than is necessary for the purpose
f) Be processed in accordance with the rights of the data subjects under the DPA
g) Be kept secure
h) Not be transferred to countries outside the EU without adequate protection

3.2 The Association and all staff who use any personal information must ensure that they follow these principles at all times. Training will be provided on the Data Protection Act and the operation of the Association's procedures in relation to the DPA & Access to Personal Information, Openness and Confidentiality and Information Security. All new staff will have this incorporated into their induction programme

3. RISK MANAGEMENT

4.1 The Association has considered the risks of the storing of personal information and recognises the possible consequences should we fail to adhere to the principles within the Act. These include being enforced to bring our practices in line with the Data Protection Action; being prosecuted by the Commission if a criminal offence has been committed, such as unlawfully obtaining personal data; being required to give compensation to an employee through the courts if damage has been caused by our failure to meet the Act.

4.2 In order to minimise risk we shall implement the Data Protection and Access to Personal Information Policy and ensure all Staff and Committee are fully aware of our requirements prior to signing the declaration.

4.3 In addition, the Association undertakes an annual risk assessment, whereby the Director assesses the risks contained within Appendix 1 a). Data Protection Audits are also undertaken where information collected/held is assessed and retained or removed as appropriate. Please refer to Appendix 1b) for the guidance on routine documents retained.

5. EQUALITY & DIVERSITY

5.1 The Association's Equality and Diversity policy, which was approved by the Committee in April 2012 following community consultation, outlines our commitment to promote a zero tolerance to unfair treatment or discrimination to any person or group of persons, particularly on the basis of any of the protected characteristics[1]. This includes ensuring that everyone has equal access to information and services and, to this end, the Association will make available a copy of this document in a range of alternative formats including large print, translated into another language or by data transferred to voice.

5.2 We are also aware of the potential for policies to inadvertently discriminate against an individual or group of individuals. To help tackle this and ensure that it does not occur, best practice suggests that organisations carry out Equality Impact Assessments to help identify any part of a policy that may be discriminatory so that this can be addressed (please see section 6 of the Equality and Diversity Policy for more information).

[1] The Equality Act 2010 identifies the "protected characteristics" as age, disability, marriage and civil partnership, race, religion or belief, gender, gender reassignment and sexual orientation.

5.3 In line with section 6.3 of the Equality and Diversity Policy, the Association will apply a screening process based on that recommended by the Equality and Human Rights Commission to ascertain whether each policy requires an Impact Assessment to be carried out. The screening process was applied to this policy and it was decided that an impact assessment is not required.

6. RESPONSIBILITIES FOR COMPLIANCE

6.1 The Director has overall responsibility for data protection within the Association, and for ensuring that our notification to the Information Commissioner, and our entry in the Data Protection Register is accurate and up to date.

6.2 The Director has specific responsibility for personal information held on employees.

6.3 The Director will perform the role of the Data Protection Officer and will assist in implementing the requirements of the Act by providing advice and support to all departments relating to compliance with the Act, disseminating information relating to the Act, and responding to requests from customers to access personal information we hold about them.

6.4 All section heads will ensure that personal data processed by their section is included in the Associations Data Protection Register entry and the entry is kept up to date and that all personal data is processed in accordance with the DPA.

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

7. TYPES OF INFORMATION

7.1 Categories

The Association is unable to categorise every type of information held on file however, they can be broken into four main categories as follows: -

1. Personal information in relation to staff, members of the Management Committee, applicants to the housing list, current tenants and former tenants, sharing owners and owner occupiers.

2. Sensitive personal information or data. In order to obtain and process personal sensitive data, the Association must obtain the individual's explicit consent.

3. Organisational information, such as measuring performance, regulator inspection reports and policies and procedures.

4. Commercially sensitive information which remains confidential under the terms of the DPA. It is acceptable to withhold commercially sensitive information provided the Association can justify it.

7.2 Sensitive Data

The DPA defines eight categories of 'sensitive data': -

1. Racial or ethnic origin
2. Political opinions
3. Religious beliefs, or beliefs of a similar nature
4. Membership of a trade union
5. Physical or mental health or condition
6. Sexual life
7. The commission or alleged commission by them of any offence
8. Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings

For obtaining and processing sensitive personal data, the Association must obtain the person's *explicit* consent for the RSL to obtain and process that particular data, unless: -

- It is necessary in respect to legally imposed employment rights and obligations
- It is already publicly available due to actions of the data subject
- It is necessary for legal proceedings, e.g. anti-social behaviour, for government or statutory functions
- It is for equal opportunities monitoring

7.3 Information Systems

Information can be held in a variety of formats, e.g.: -

- Databases
- Spreadsheets
- Manual records, files, card indexes
- Computerised files and records
- E-mail - The Association processes information which identifies individuals via e-mail correspondence. In order to minimise the risks associated with this, and in accordance with guidance, the following disclaimer is contained within each staff members' e-mail 'signature': -

  This electronic message and any associated files transmitted with it are confidential and intended solely for the use of the person to whom or which it is addressed. You are hereby notified that if this message contains personal or commercially sensitive information, any dissemination, copying or distribution of the information is strictly prohibited. Irrespective of the contents, if you are not the intended recipient please contact the sender and delete this message. Any representations, contractual or otherwise, views or opinions presented are solely those of the author and do not necessarily represent those of Cernach Housing Association Limited.

  As part of Cernach Housing Association Information Security and Data Protection Policy the Association monitors e-mail content. The Association has anti virus software installed and all applications are scanned for known viruses. The Association cannot accept responsibility for viruses, so please scan attachments.

- CCTV - The Data Commissioner has been formally notified of the installation of CCTV equipment within the Association's stock in 2006. In accordance with guidance, notices have been erected throughout the stock base affected and only authorised personnel are able to access the data room where CCTV images can be viewed. A log of any reviews is maintained by appropriate staff and regular integrity checks are undertaken.

8. CONFIDENTIALITY

8.1 This Policy complements the Associations Openness and Confidentiality Policy. Only information which can or must be legally disclosed under the DPA will be shared with a third party without the individuals consent.

8.2 Employees and Committee members will be obliged to sign a confidentiality form and to agree to the security measures to ensure the security of personal information against unlawful processing, disclosure, accidental loss or destruction of, or damage to, personal data.

8.3 All staff will have a password to ensure information is only accessible to those who need to know the information in order to carry out their requirements of their post.

9. COMPLAINTS

9.1 Should any applicant be dissatisfied with the way their data access application has been dealt with they may complain to the Data Protection Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF Telephone 01625 545 700

9.2 Where applicants are dissatisfied with the way their request for personal information has been dealt with and it falls out with the scope of the Data Protection Act, they should make a complaint in accordance with the Associations Complaints Policy. Ultimately, and following exhaustion of the Complaints Procedure, they may apply to the Scottish Public Services Ombudsman, 4 Melville Street, Edinburgh, EH3 7NS, Telephone 0870 0115378 or e-mail enquiries@scottishombudsman.org.uk.

10. BREACHES OF POLICY

10.1 Section 12 outlines the procedures to be followed when dealing with personal information requests. Any breaches of the Data Protection & Access to Personal Information Policy & Procedure shall be taken seriously by the Association and appropriate action taken against either Staff or Committee member(s) involved.

11. POLICY REVIEW

11.1 The Data Protection & Access to Personal Information Policy & Procedure shall be reviewed every three years or sooner as deemed necessary by the Management Committee. The success of the policy shall be measured against the following outputs and outcomes: -

OUTPUTS	OUTCOMES
Appropriate procedures in place, in line with legislation to assist Staff in dealing with requests	*Applications for personal information successfully handled*

12. PROCEDURES

12.1 Introduction

The Association conducts its affairs openly and will respond openly to requests for information, unless there are justifiable reasons for withholding it. There is a separate Openness and Confidentiality Policy, which covers this.

This procedural note refers to the Data Protection Act (DPA) and the steps the Association must take to ensure compliance with the Act and to implement the Association's Policy in relation to the DPA and access to personal information.

12.2 Registration And Changes To Notification

The Association has registered with the Information Commissioner and this registration is renewed on an annual basis.

The Data Controller shall notify the Information Commissioner of any changes to the list of purposes for which we process data within 28 days.

12.3 Access Rights

a) Tenants, prospective tenants, employees and other individuals about whom the Association holds personal information have the right to access the information, unless it is exempt under the DPA. This should be done in writing by the 'data subject' to the Director who shall acknowledge receipt of the request within 2 working days. (Please refer to Appendix 2 for a sample 'Subject Access Request Form'). A computerised register of requests is stored on the server and is maintained by the Director

b) Within a further 10 working days the Director shall undertake an assessment of the request and respond to the data subject in writing. (Please refer to Appendix 3 for a sample 'Checklist for Assessing Requests for Personal Information').

c) In general terms an individual should be given all the personal information held about them on request and ask that any inaccurate information be removed or corrected.

The data subject will be told whether personal data is being processed and the description of what data is being processed, why and to whom that data may be disclosed and the source of the data UNLESS: -

- Release of the information would prejudice the prevention or detection of crime
- it identifies someone else who objects to being identified
- it is confidential because it was provide din the context of a lawyer-client relationship
- it would involve 'disproportionate effort'. In this case the data subject need only view the data in its original form at the Association's office.

d) The Association will respond to information requests within 40 days of receipt of sufficient information to enable the required data to be located.

e) The Association will charge the recommended fee for providing access to data. This is currently £10.00 and the 40 day response time shall commence once the fee is paid and appropriate identification evidence has been provided.

12.4 Conditions Relating to Processing Data Lawfully

a) All personal data must be processed in a fair and lawful manner. Processing is lawful when one of the following conditions are met: -

- The data subject has given the explicit consent to the way in which it is proposed their personal data is to be processed.

- Silence cannot be taken as consent. The most obvious way of doing this would be by obtaining the persons signature on a form with the relevant details printed there and a statement as to what it will be used for.

b) The following are examples of some areas where we should obtain the consent of the data subject: -

- **Tenancy Agreements** – A clause should be added advising that we will process data and pass to relevant agencies and for court action
- **Housing List** – Applicants are asked to sign a declaration that we can ask for previous tenancy information
- **Special Needs** – Tenants are asked to authorise the Association to provide information to their provider
- **Recruitment** – Applicants are asked to sign a declaration that we can apply for references for them
- **Employees Personal Information** – Employees are asked to agree that information on absences, appraisals, etc. can be reported to Committee
- **Pensions Trust** – Employees are asked to agree that we can process information to the Pension Trust on their behalf
- **Committee Members' Personal Information** – Committee members are asked to agree that we provide personal information to FSA, OSCR and the Scottish Housing Regulator
- **Confidentiality Clauses** – Any third parties who process or has access to personal information held by the Association shall have a declaration contained within the contract confirming their compliance with the Data Protection Act, e.g. CNS2000 and SDM.
- The processing is necessary for the purposes of a contract involving the data subject.
- The processing is necessary to protect the vital interests (life or death) of the data subject, where he/she cannot give consent or the consent cannot be reasonably obtained.
- The processing is necessary to protect the vital interests of another person and the data subject unreasonably refuses consent.
- The processing is necessary for the purposes of legal proceedings, taking legal advice, or establishing, exercising or defending legal rights or for the administration of justice. Accordingly disclosure of sensitive, personal data in the context of an anti-social behaviour court case is permitted as long as it is necessary.
- The data subject has already deliberately made the information public

c) Where the Association is uncertain as to whether an exemption applies the Information Commissioner should be consulted.

12.5 Recruitment Records

a) All recruitment adverts shall contain the Association's full registered name, address and contact details of the specified member of staff authorised to administer the responses.

b) The Association shall only use the information contained within the applications received for the purposes of recruiting for the post advertised and the application form shall inform the applicants that the forms shall be retained for the period outlined in the Data Protection & Access to Personal Information Policy & Procedure.

c) Information about criminal convictions in line with the Rehabilitation of Offenders Act 1974 shall be requested at the time of applying for the post. This shall be followed up with a questionnaire to those candidates who are called to interview. This information shall be retained in line with the Data Protection & Access to Personal Information Policy & Procedure.

d) Where criminal conviction information is required to be verified, the Criminal Records Bureau (CRB) shall be contacted, and their procedures followed. Any detailed information provided shall not be retained, however, a note of whether it was satisfactory or unsatisfactory shall be recorded in the file.

e) A health questionnaire shall be issued to successful applicants only. It shall be noted on the form that the information shall be retained in line with the Data Protection & Access to Personal Information Policy & Procedure.

12.6 Personnel Records

a) At the time of commencing employment, staff are requested to complete a personal record sheet. This provides information on contact details, next of kin (emergency contact), pension, salary and annual leave entitlement and is accessed by the Director, the HSM and Finance Officer. This information is retained within the locked personnel filing cabinet and destroyed after employment ceases in line with Data Protection & Access to Personal Information Policy & Procedure.

b) At least on an annual basis, staff are requested to complete an equal opportunities monitoring form. This is to monitor ethnicity, disability, gender and age within the organisation and is only used for statistical purposes. This information is not stored in individual personnel files.

c) Sickness absence sheets shall be retained in staff personnel files for monitoring purposes and reported on a quarterly basis to the Management Committee. The statistical information shall also be used when completing the ARC and benchmarking groups that the Association participates in. The tear off slip at the bottom of the absence sheet is designed to provide minimum information to the Finance Officer to allow the SSP to be calculated for the absence(s). These are stored with the salary information in a locked cabinet.

d) Personnel files shall be kept up to date by the Director and contain information relating to salary, pension, training and development, appraisals and any disciplinary a correspondence. With the exception of the disciplinary correspondence, which shall be held on file for the period outlined within Disciplinary Policy & Procedure, all other data shall be retained for the period defined within the Data Protection & Access to Information Policy & Procedure.

e) Staff may request access to their personnel file and this should be done in writing to the appropriate Line Manager. This shall be responded to within ten working days. The file may not be removed and shall be reviewed in the Director's office.

12.7 Employment References

12.7.1 Writing a Reference for an Employee

References written about staff members shall be held in their personnel file, however these will not be disclosed to Staff, other than the facts that they will already be aware of.

12.7.2 Receiving a Reference

References provided from other employers may be disclosed to the staff member, however, the author will not be identified and the referee will be contacted to find out if they object to the information being divulged. If so, only the facts (rather than opinions expressed) can be provided to the staff member.

12.8 Sharing Information With Other Agencies

a) No employee may pass on personal information held on any individual to a third party without the individuals' consent, unless it is necessary disclosure of information in connection with legal proceedings, or the administration of justice.

b) The arrangements for sharing information between agencies should be clearly defined in a joint protocol to ensure that the amount of information exchanged is compatible with the DPA. This protocol should state that any information disclosed remains the property of the disclosing agency and only used for the purposes it was requested for and used only by the agency requesting the information.

c) If the Association seeks to use the information for another purpose or seeks to disclose the information to another third party, then the disclosing agency must be contacted to give their approval of the disclosure. If for instance, the Association requests information on Mr Nobody who is a tenant of the Association and the police disclose information on a number of incidents at the property involving Mr Nobody. Mr Nobody then asks the Association for access to his house file. The Association must therefore contact the police to seek formal approval to disclose this information to Mr Nobody as this information cannot be disclosed with the police agreement to disclose the information to Mr Nobody.

d) The Scottish Housing Regulator has a right to access personal information from either personnel or tenant files for the purposes of inspection. The Scottish Housing Regulator is listed on the Association's notification to the Information Commissioner as a third party and therefore in line with the 1st principle are exempt. Individuals are not required to give their consent before this information is released.

12.9 Security Measures To Safeguard Personal Information

a) Whilst the Association has a separate Information Security Policy, which is signed by all staff, the Data Protection & Access to Personal Information Policy & Procedure is signed by members of staff and Committee. By doing so, they agree to adhere to the measures in place to ensure security of personal information against unlawful processing, disclosure, accidental loss or destruction of or damage to personal data (in line with 7th principle of DPA).

b) All staff are given a password for specific access to the computer server files and a separate password to access the SDM housing management system. The passwords will limit access according to job role. Some users may only need to have 'read only' access to certain information and be denied access to other information altogether.

c) Access to information will generally be on a 'need to know' basis and is consistent with good practice for maintaining confidentiality and to protect against unauthorised or unlawful processing and/or accidental loss or destruction of or damage to data. Under no circumstances should electronic information stored on the Association's equipment be deleted without the express permission of a member of the Management Team.

d) Passwords will be changed at regular intervals and a written procedure will set out who is authorised to access which records and for which purpose. Passwords should not be disclosed. Daily back-up of information is made and disks are checked for virus on the laptop before use. The Association has anti-virus software installed which checks files on the network and this is regularly checked by the IT Contractor, as is the back-up integrity.

e) It is not permissible to install any software not licenced to the Association and this includes screen savers, games and free software from, for example, magazines.

f) Staff should not leave personal information on their desk unattended nor access systems to check personal information for themselves. Particular care should be taken in public areas and interview rooms to position the monitor to avoid casual browsing. In particular, care should be taken to ensure the screen is locked before exiting an interview room.

g) All personal information being disposed of must be disposed as confidential waste using the Association's shredder.

13. STAFF AND COMMITTEE DECLARATION

I am fully aware and understand the contents of the Association's Data Protection and Access to Personal Information Policy and agree to maintain the confidentiality of all personal information disclosed to me as part of my role as a staff/committee member. It is understood that the Association holds and processes personal information on me and by signing this declaration agree that the Association can provide specific information to third parties as required by Regulatory bodies, Employment legislation or Pensions Trust.

Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	
Signature		**Date**		**Signature**		**Date**	

Cernach Housing Association
Data Protection and Access to Personal Information Policy & Procedure

APPENDIX 1 a) – RISK MANAGEMENT

RISK ASSESSMENT CRITERIA

1.	Does the Association have an Information Security Policy that has been signed by all Staff?	**YES** ❑ **NO** ❑
2.	Have all staff been issued with passwords for PC and SDM?	**YES** ❑ **NO** ❑
3.	Are staff aware of the restrictions to directories/documents stored on the server?	**YES** ❑ **NO** ❑
4.	Are staff aware that they should save all documents onto the server rather than on local disk drive (failure to do so would result in information not being backed up)?	**YES** ❑ **NO** ❑
5.	Do staff lock their computer when away from their desk?	**YES** ❑ **NO** ❑
6.	Are staff aware they should avoid sending confidential information via e-mail?	**YES** ❑ **NO** ❑
7.	Is there a disclaimer attached to each staff members' outgoing e-mails?	**YES** ❑ **NO** ❑
8.	Have computers been situated where it is difficult for visitors to see the screen?	**YES** ❑ **NO** ❑
9.	Are software disks and registers stored in either the fire proof safe or the multi-media safe?	**YES** ❑ **NO** ❑
10.	Is there a daily back-up taken of the server documents and SDM?	**YES** ❑ **NO** ❑
11.	Is the integrity of the back-up checked regularly by the IT contractor?	**YES** ❑ **NO** ❑
12.	Is all information stored in lockable cabinets where possible?	**YES** ❑ **NO** ❑
13.	Is all personal information on paper destroyed either by shredding or sending to a specialist company?	**YES** ❑ **NO** ❑
14.	Have staff and committee received a full copy of the Data Protection & Access to Personal Information Policy & Procedure and signed to confirm their knowledge and understanding?	**YES** ❑ **NO** ❑
15.	Does the Association have a Disaster Recovery Plan in place?	**YES** ❑ **NO** ❑

Where 'No' is ticked at any of the above, details should be appended outlining how it will be overcome. This and any supporting documentation shall be completed and filed by the Drector in the Data Protection folder in the central storage system.

Signed: _____ Date: _____

APPENDIX 1 b) – RISK MANAGEMENT

INFORMATION AUDIT – PERSONAL DATA

WHEN CARRYING OUT THE AUDIT THINK: -

What is done with this information?	Why is it needed?
When was it stored or last updated?	Is it correct and up to date?
Is there duplication with other information held?	Is there justification for keeping the information?

Name: …… **Department:** **Human Resources/Corporate Services**

Detail of Information Collected or Held	Location	Purpose Collected or Held	Period Retained For	Exchanged with/Passed onto
Employees' personnel records	Locked cabinet. Personnel computer records	Details of employment and next of kin, etc. for efficiency of organisation	While in employment (except spent disciplinary matters)	Details supplied for references, Inland Revenue, Police, Pension Scheme, DSS, Department of Employment, Auditors, SHR, Solicitors, Employee Counselling Service
Past Employees' personnel records	Archive boxes in attic	Reference for future employers, Pension companies	6 years after employment ceased	Other employers, Pensions, Police, Inland Revenue, DSS, Department of Employment, Auditors, SHR, Solicitors
Unsuccessful job applicants' application forms	Archive boxes in locked cabinet at central filing area	In case of dispute/ Industrial Tribunal or query on application	12 months	ACAS, Industrial Tribunal, Lawyers acting for the RSL
Accident or injury at work records	Health & Safety File in central storage system	In case of claims	12 years	Insurers
Membership details – name and address	Computer database and manual records in locked cabinet at central filing area	Statutory obligation	Indefinitely	Auditors, SHR, publicly available document
Committee members names, address, date of birth and code of conduct details	Lever arch file and computer records	Regulatory requirement	While a Committee member and 6 months after financial year end	Names included in Business Plan and circulated to anyone, Auditors SHR

APPENDIX 1 b) – RISK MANAGEMENT

INFORMATION AUDIT – PERSONAL DATA

WHEN CARRYING OUT THE AUDIT THINK: -
What is done with this information? Why is it needed?
When was it stored or last updated? Is it correct and up to date?
Is there duplication with other information held? Is there justification for keeping the information?

Name: …… Department: Human Resources/Corporate Services (Cont'd)

Detail of Information Collected or Held	Location	Purpose Collected or Held	Period Retained For	Exchanged with/Passed onto
Telephone contacts, addresses and e-mail addresses of suppliers, contractors and other contacts	Telephone directories, address books (manual and computerised (e.g. LOAC))	To be able to contact people	Indefinitely	Anyone who asks
Benefits given to staff/Committee	Payments & Benefit to Staff & Committee Register	Openness and accountability	Indefinitely	Publicly available record and reported to Committee twice a year.
Complaints to the RSL and the Ombudsman	Computerised with hard copy stored in lever arch file in central filing area and archive box in attic	To monitor and record complaints	Indefinitely	Ombudsman, Committee, Auditors, SHR, other staff, tenants via newsletters (anonymous statistics only)

APPENDIX 1 b) – RISK MANAGEMENT

INFORMATION AUDIT – PERSONAL DATA

WHEN CARRYING OUT THE AUDIT THINK: -
What is done with this information? Why is it needed?
When was it stored or last updated? Is it correct and up to date?
Is there duplication with other information held? Is there justification for keeping the information?

Name: …… Department: Housing Management

Detail of Information Collected or Held	Location	Purpose Collected or Held	Period Retained For	Exchanged with/Passed onto
Right to Buy and Shared Ownership & Owners details	Section 9 register	Statutory obligation	Indefinitely	SHR, publicly availably document
Housing applications	Lateral hanging files in lockable cabinet	To allocate houses fairly	Until allocation made or cancelled. If allocation made, remains in tenant file until they become a former tenant	SHR & Committee (statistics only)
Ethnic monitoring forms for housing list applications	Lateral hanging files in lockable cabinet	Reporting for ARC & Committee	Removed annually	Auditors, SHR and Committee (statistics only)
Cancelled housing applications	Lateral hanging files in lockable cabinet	To streamline housing list as historically applicants will respond some time after cut off period	6 months after date of cancellation	Committee (statistics only)
Tenant Files & Rent Account	Central storage system & SDM	To record rent payments, arrears and HB arrangements & to produce reports as well as record any other activity during tenancy	Until tenancy ends and then moved to F/T status	SHR, Auditors, Solicitors, Welfare Benefits Advisor, HB
Former Tenant Files	Archive box	To refer to in relation to tenancy reference requests from new landlords. Right to Buy applications. There shall be a summary sheet prepared outlining tenancy details (RTB status, DOE, DOL, ASB incidents, rent account activity and any outstanding debt (rent and/or re-chargeable repairs))	Indefinitely	Other landlords
Anti-social complaint records	Individual tenant files and register	Central storage system and lockable cabinet	Annual clear out	SHR, Auditors, Solicitors
Disabled Adaption files	Lever arch file in lockable cabinet, property file & SDM	To keep accurate record of adaptations made	Indefinitely	SHR, Social Work, Contractors

APPENDIX 1 b) – RISK MANAGEMENT

INFORMATION AUDIT – PERSONAL DATA

WHEN CARRYING OUT THE AUDIT THINK: -

What is done with this information? Why is it needed?
When was it stored or last updated? Is it correct and up to date?
Is there duplication with other information held? Is there justification for keeping the information?

Name: …… Department: Maintenance

Detail of Information Collected or Held	Location	Purpose Collected or Held	Period Retained For	Exchanged with/Passed onto
Repairs work orders & satisfaction surveys	Lever arch file, property file on SDM	To keep record of individual repairs carried out in each property and for statistical reports	7 years	SHR, Auditors
Insurance claims	Lever arch file and on server	To monitor claims	7 years	Auditors, Insurers
Re-chargeable Repairs	Lever arch file, SDM & server	To record payments due and paid and action taken	7 years after debt cleared or written off	Auditors, Other landlords (tenancy reference)
Gas Safety Certificates	Lever arch file, SDM & tenant file on server	Legislative requirement for last two years for each property	7 years	Auditors, SHR

APPENDIX 1 b) – RISK MANAGEMENT

INFORMATION AUDIT – PERSONAL DATA

WHEN CARRYING OUT THE AUDIT THINK: -
What is done with this information? Why is it needed?
When was it stored or last updated? Is it correct and up to date?
Is there duplication with other information held? Is there justification for keeping the information?

Name: …… Department: Finance

Detail of Information Collected or Held	Location	Purpose Collected or Held	Period Retained For	Exchanged with/Passed onto
Invoices	Locked cabinet	Auditing purposes	7 years	Accountant, Auditors and SHR
Salary information	Locked cabinet	Auditing purposes	7 years	Accountant, Auditor

APPENDIX 2

Cernach Housing Association
Data Protection Act 1998
Subject Access Request Form

The Data Protection Act 1998 entitles you to ask for a copy of any personal information we hold about you. In addition to the information itself, you are entitled to be told why we have the information, to whom we disclose it and where we obtained it from.

This form will assist you in making a request for that information. You do not have to use it, but it will help us to help you if you do so. If you choose not to use the form, any request for information must still be in writing.

If you need help completing the form, the Association can help you do this – we can fill out the form on your behalf and read it back to you before asking you to sign it.

1. Details of the person requesting the information

Full Name _____

Address _____

Tel No. _____

E-mail _____

2. Are you the data subject? (this means are you the person about whom the information is being requested)

Please tick yes or no below, and remember to enclose the documents requested. Please do not send original documents through the post, unless you use registered post. If you bring original documents to the office, we will make a copy and return the originals to you.

- ❑ **YES**: I am the Data Subject and I enclose a form of identification. (acceptable forms are originals or photocopies of a birth certificate, driving license, National Insurance or NHS card). **If you answered YES, please go to question 4**
- ❑ **NO**: I am NOT the Data Subject but I am acting on behalf of him/her with written authority to do so. (Please enclose the original of the written authority and a form of identification for the Data Subject – i.e. a birth certificate, driving license, National Insurance or NHS card). **If you answered NO, please complete question 3**

3. Details of the Data Subject? (i.e. the person whose personal information you are requesting (if different from question 1)

Full Name _____

Address _____

Tel No. _____ E-mail _____

Please say briefly in the space below why you are seeking information on behalf of someone else.

4. Please describe the information you want as clearly as possible in the space below (for example, do you want to see a specific piece of information, or do you want to know what information we hold about you?)

Declaration (to be completed by ALL applicants)

I certify that the information given on this form is accurate and true. I understand that it is necessary for Cernach Housing Association Ltd. to confirm my identity and that of the Data Subject (if different from myself) and that it may be necessary to obtain more detailed information in order to comply with this application.

Signature: _____ Date: _____

Notes

- We are allowed to charge up to £10.00 for each application. We will advise you no later than 10 working days after receiving your request whether any charge will be made.
- We shall respond to you within 40 days and this period will not begin until we have received satisfactory proof about your identity and that of the Data Subject (if different) as well as the fee if chargeable.

Please return this completed form and supporting information to: -
Jean Thomson, Director
Cernach Housing Association Ltd.
79 Airgold Drive
Drumchapel
GLASGOW
G15 7AJ

APPENDIX 3
CHECKLIST FOR ASSESSING REQUESTS FOR PERSONAL INFORMATION

In dealing with requests for access to information under the Data Protection Act, Staff should complete the following pro-forma to record the action they have taken.

	Comment/Action
1. Name of Applicant	
2. Date of completed access request form (Appendix 2), or other written request from data subject **Provide assistance with form completion if needed:** - Fill out form on data subject's behalf - Read the form back to them - Ask data subject to sign and provide them with a copy	
3. Confirm within 10 WORKING DAYS a) Satisfactory proof of identity provided? b) Satisfactory evidence of authority, if application submitted on data subject's behalf? c) Is it clear exactly what information is being requested? **IF YES** – No action required **IF NO** – write to applicant within 10 working days reminding them that 40 day period for dealing with request only starts when information provided. Acceptable forms of proof of ID and evidence of authority are a birth certificate, driving license, NI or NHS card – or any other definitive form of identification. Passports are acceptable if volunteered by the applicant but should NOT be requested by CHA. Place copies of proof of ID (and evidence of authority if applicable) on file	

	Comment/Action
4. Is the request likely to be unusually onerous? (e.g. excessive staff resources required for data gathering, copying) **IF NO** – no action required **IF YES** – a) Director to confirm whether a charge should be made (maximum £10 per request) b) Director to confirm whether data subject to be advised that they may inspect information at the office, rather than have copies made by CHA. c) Write to applicant confirming if a charge is to be made or not d) Write to applicant if CHA will allow inspection of data at office but will not provide copies because of resources required (letter to give Information Commissioner's Office contact details) **Charging and refusal to provide copies is likely to be exceptional and should be authorised by Director.**	
5. Within 40 days of a completed application: Confirm that the Data requested falls within the DPA (seek advice from solicitors or Information Commissioner if the request is non-routine/likely to be refused/there is any doubt about the data subject's legal entitlements) **Otherwise, check: -** **a) If the request is for a specific piece of information:** - It is personal information relating to the individual - The information is held on computer or on paper and sorted by reference to individuals - Providing the information will not breach the confidentiality of another individual. If other individuals are named or could be identified from the data requested, refer to the decision flowchart attached to aid decision-making (Appendix 4). **b) If the request is for a description about what persona data CHA holds about the data subject:** - Prepare a description in accordance with legal requirements. For example: - 1. A description of the personal data which is held by CHA 2. A description of the purposes for which CHA processes/uses the data 3. A description of the recipients or the classes of recipients to whom the data my have been disclosed 4. Explanation of any jargon or technical terms	
6. Issue formal response to data subject as soon as possible and within the 40 day time limit	
7. Confirm here the date the formal response was issued by CHA	

APPENDIX 4

DATA REQUESTS WHICH INCLUDE INFORMATION ABOUT A THIRD PARTY
DECISION FLOW-CHART