Data and Information Management

Policy and Procedures

Contents

1 Introduction

As an organisation, West of Scotland Housing Association manages a significant amount of data and information. Much of this data and information is sensitive personal information relating to staff and tenants. Therefore it is essential that all staff and volunteers within the organisation are aware of the importance of managing this data and information effectively and carry out their responsibilities in this respect.

The purpose of this document is to convey West of Scotland Housing Association's policy and procedures for the management of data and information and consequently to give staff and volunteers guidance on the effective management of data and information.

It details guidelines for West of Scotland Housing Association information handling, subject access to records and creation and management of records including retention and disposal of records.

Why should West of Scotland Housing Association manage and protect data effectively?

- It is a legal requirement (Data Protection Act 1998 and Human Rights Act 1998)
- It is essential that we respect the rights of our Tenants and staff and that they can trust us to manage and protect their information effectively.
- It makes good business sense. For example:
    - ✓ Sending out mailing from incorrect or out of date records could waste time and money
    - ✓ Good information handling can enhance the organisation's reputation by increasing stakeholder and employee confidence
    - ✓ Good information handling should reduce the risk of a complaint being made against the organisation
    - ✓ In order to run effectively as an organisation, it is important that we have systems, structures and processes in place to ensure the management and protection of information.
- If an individual suffers damage as a result of the organisation not working in line with data protection requirements, then that individual may seek compensation for the damage through the courts.

What happens if West of Scotland Housing Association does not manage and protect data effectively?

- Tenant or staff information could be lost, destroyed or used inappropriately.
- The association's reputation could be badly damaged
- The association's finances could be affected
- The Information Commissioner could take enforcement action against the organisation to bring processing into compliance with the principles of the Data Protection Act 1998, this could mean a fine for the organisation
- An individual may seek compensation through the courts for any damage

Policy Statement

- West of Scotland Housing Association is committed to ensuring that all data and information within the organisation is managed efficiently particularly in relation to staff and tenant information.
- West of Scotland Housing Association is committed to complying with all legislation relating to the management of data and information.
- All West of Scotland Housing Association staff and volunteers have a responsibility to ensure that data and information is managed effectively within the organisation.

2 West of Scotland Housing Association Data and Information Management Standards

- All data and information that we hold regarding staff or tenants should be collected fairly within legal requirements.
- All data and information that is collected and held regarding an individual should be relevant to the purpose and should not be excessive or irrelevant.
- All data and information held should be arranged in a structure that will enable quick and easy retrieval of information.
- All data and information that we hold regarding staff or tenants, hard copy or electronic copy, should be stored securely as per policy and procedures.
- A clear desk policy should be implemented in all WSHA bases, desks should be cleared at the end of the working day and any sensitive information should be locked away.
- Storage of current and archived data and information held within offices should be clean, tidy, clearly labelled to prevent any damage to records.
- Access to tenant and staff information should be on a “need to know” basis within WSHA e.g. a key worker will require to access to information regarding a tenant that they are supporting but the administrator may not require access to this information.
- Equipment for storing data and information should prevent unauthorised access and meet fire and health and safety requirements.
- We should only share staff or tenant information with third parties on a “need to know” basis and where we have consent from the individual. There are exemptions to this which are detailed in this policy.
- All departments should have a process in place to allow tenants to access information held about them. Staff would contact HR directly to access their own information. There are exemptions where WSHA would refuse access – these are detailed in the policy.
- All data and information stored regarding an individual should be accurate and up to date.
- Data and information regarding an individual should not be kept longer than necessary (See Retention Guidelines)
- All departments should review data and information held on individuals on an annual basis and archive/destroy where appropriate.
- Information and data should be archived securely and within timelines as per the policy and procedures
- The destruction of data and information should be done securely as per policy and procedures.

3 Relevant Legislation

Human Rights 1998

The Human Rights Act 1998 came into force in October 2000. It gives effect to the European Convention on Human Rights 1950, which now becomes directly part of our law.

Article 8 of the Convention gives everyone the right to respect for their private life, their home and their correspondence.

West of Scotland Housing Association must respect this right in all our actions including when gathering and processing information relating to individuals.

By ensuring proper procedures are put into place, West of Scotland Housing Association will be able to show that staff and tenants' rights of privacy are being respected.

Data Protection Act 1998

The Data Protection Act came into effect on 1st March 2000.

The Act defines a legal basis for the handling of information relating to people. It aims to promote high standards in the handling of personal information, to protect the individual's right to privacy.

The Data Protection Act works in two ways:

- It says anyone who records and uses personal information (data controllers) must be open about how the information is used and must follow eight principles of good information handling (see below)
- It gives us all as individuals (data subjects) certain rights including the right to see information that is held about us and to have it corrected if it is wrong.

The Data Protection Act covers electronic and manual records such as those recorded on paper or other media such as pcs, laptops, pen drives etc and is concerned with the processing of 'personal data', that is data relating to identifiable living individuals.

The Data Protection Act enhances the rights of data subjects in gaining access to information about themselves and if organisations such as West of Scotland Housing Association ensure that they have well maintained records they will find it easier to comply with the requirements of the Act.

Eight Principles of good information handling

All staff and volunteers handling 'personal data' must follow the 8 data protection principles.

The first five principles establish general standards of data quality. They specify that data must be:

- Obtained and processed fairly and lawfully
- Held only for specific and lawful purposes and not processed in any matter incompatible with those purposes
- Relevant, adequate and not excessive for those purposes
- Accurate and where necessary kept up to date
- Not kept for longer than is necessary

The sixth principle says that data should be processed in accordance with the rights of data subjects under this Act. This means that individuals have the right, amongst other things to:

- Be informed upon request of all the information held about them by a particular data controller.
- Prevent the processing of their data for the purposes of direct marketing
- Compensation if they can show that they have been caused damage by any contravention of the Act
- The removal or correction of an inaccurate data held about them.

The seventh principle requires you to ensure that you have adequate security precautions in place to prevent the loss, destruction or unauthorised destruction of the data.

The eight principle requires you not to transfer data outside the European Economic Area unless you are satisfied that the country in question can provide an adequate level of security for that data.

Notification

The Information Commissioner maintains a public register of data controllers. The data protection register is published on the internet.

West of Scotland Housing Association is registered with the Information Commissioner as a data controller and this registration is renewed on an annual basis.

4 Role of the Information Commissioner

The Information Commissioner's office (ICO) is the UK's independent public authority set up to uphold information rights. They do this by promoting good practice, ruling on complaints, providing information to individuals and organisations and taking appropriate action when the law is broken.

There are a number of tools available to the ICO for taking action to change the behaviour of individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to service a monetary penalty notice on a data controller.

The Information Commissioner is appointed by the Queen and reports directly to Parliament. The Commissioner is supported by the management board.

5 Policy Links

This policy should be read in conjunction with the following West of Scotland Housing Association Policies:

- IT Policies and Procedures
- Section C1 Terms and Conditions of Employment – Code of Conduct
- Section C2 Terms and Conditions of Employment – Personal Information
- Code of Conduct Policy
- Secure Handling, Use, Storage and Retention of Disclosure Information Policy
- Staff Code of Conduct Policy

6 Dealing with Breaches

If a breach of security in relation to personal information occurs, it is important that it is dealt with effectively. The breach may arise from theft, a deliberate attack on systems, from unauthorised use of personal data by a member of staff or from accidental loss or equipment failure. Staff should report the loss or theft of personal information to their line manager with immediate effect.

There are four main elements to a breach management plan:

1. Containment and recovery – the response to the incident should include a recovery plan and, where necessary, procedures for damage limitation.
2. Assessing the risks – you should assess any risks associated with the breach, as these are likely to affect what you do once the breach has been contained. In particular, you should assess the potential adverse consequences for individuals; how serious or substantial these are and how likely they are to happen.
3. Notification of breaches – informing people about an information security breach can be an important part of the incident, but it is not an end in itself. You should be clear about who needs to be notified and why. You should consider notifying the individuals concerned; relevant regulatory bodies; other third parties such as the police, the banks or the media.
4. Evaluate and response – it is important that you investigate the causes of the breach and also evaluate the effectiveness of your response to it. Depending on the circumstances surrounding the breach, if there is a direct non-compliance of policies and procedures e.g. Code of Conduct by a staff member(s) or volunteer, the disciplinary procedure should be followed by HR.

Reporting breaches to the Information Commissioner

All breaches should be reported to the Director of Finance and Corporate Services and Corporate Services Manager and they will determine the seriousness of the breach. Although there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his office. The nature of the breach or loss can then be considered together with whether the data controller is properly meetings his/her responsibilities her under the Data Protection Act.

Serious breaches are not defined. However, the following will assist us to consider if a breach should be reported:

- The potential detriment to data subjects. Detriment includes emotional distress as well as both physical and financial damage. Ways in which detriment can occur include:

    - ✓ Exposure to identity theft through the release of non-public identifiers e.g. passport number;
    - ✓ Information about private aspects of a person's life becoming known to others e.g. financial circumstances, criminal history etc

The extent of the detriment likely to occur is dependent on both the volume of persona data and the sensitivity of the data.

- The volume of personal data lost/released/corrupted. There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm.
- The sensitivity of data lost/released/corrupted. There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause significant risk of individuals suffering substantial detriment.

Please note that a verbal disclosure constitutes as a breach as well as written or electronic information e.g. if you verbally disclose personal sensitive information regarding an individual which falls into the above categories.

Any potential breaches should be reported to the relevant Manager and OD Officer before reporting to the Information Commissioner. An investigation will then be carried out to determine the nature of the breach and whether it should be reported externally.

A central record will be kept of all breaches both reported and non-reported by the Corporate Services Manager.

7 Consent

Tenant Information - Sharing records and information with external agencies

You need permission from the individual before you can share the information that you hold regarding them with external agencies.

You must not share information regarding a tenant if they have not given permission to share information with that individual/agency or if they have specifically stated that they do not want information shared with a particular individual or agency.

Please note for the purposes of the data protection legislation any subsidiary of WSHA is considered as an external agency and consent is required.

Staff Information – Sharing records and information with external agencies

The information and records held regarding staff are held for WSHA use only and should only be accessed by WSHA staff on a 'need to know' basis. West of Scotland Housing Association does not have the permission of staff to share records and information with external agencies, therefore if a request is made, they must get written permission from the staff member for that information to be shared by that particular agency or organisation.

Where permission is not required

Permission to share information is not required for staff or tenants in the following circumstances:

- Where there is an obligation to report a crime.
- Where there is a serious risk of suicide, violence or abuse, especially to a child or young person.
- Where disclosure is legally required (statute or court).
- Where urgent medical attention is required.
- Where considerations to public interest outweigh other considerations.

If any of the above apply, the relevant authority e.g. police, that requires the information should complete should supply you with a written document confirming that they have requested this information so that you have documented proof of the information being taken away or shared.

8 Access to Records

Individuals have a right under the Data Protection Act to make a request in writing for a copy of information held about them on computer and in manual filing systems. This is called a subject access request.

Individuals making a subject access request are entitled to a copy of the information held about them, both on computer and manual filing systems. They also have the right to receive a description of why their information is being held, anyone it may be passed to, and information about the source of information.

WSHA must respond to a subject access request within 40 calendar days from receipt of request. The relevant Manager should deal with any subject access requests.

If a fee is required, or if further details such as clarification of the query or confirmation of the person's identity are needed, the 40 calendar days will begin when these are received.

In cases where West of Scotland Housing Association receives a data subject request but doesn't hold the information requested, the applicant must be informed as quickly as possible.

Routine amendments and deletions to personal information can still be made after receiving a request. However, you must not make any changes to the records as a result of receiving the request, even if you find inaccurate or embarrassing information on the record. When recording information regarding tenants or staff, staff should be aware that individuals have the right to access their records, therefore records should always be accurate and professionally written and sensitivity should be shown where required.

A copy of the information held can be issued as a computer printout, in a letter or on a form. It should be easy to understand and if any codes are used these should be explained.

Where it would be impossible or would involve significant cost or time taken to provide information in hard copy, the applicant may be allowed under supervision to examine the information held about them in a computerised or manual filing system; providing the applicant consents to this.

There may be circumstances in which you are not obliged to supply certain information. Some of the most important exemptions apply to:

- Crime prevention and detection
- Negotiation with the requestor
- Management forecasts
- Confidential reference given by you (but not ones given to you)
- Information used for research, historical or statistical purposes
- Information covered by legal professional privilege

If the subject's data includes information on other people you will not have to supply the information unless the other people mentioned have given their consent, or it is reasonable to supply information without their consent. Even when the other person's information should not be disclosed, you should still supply as much as possible by editing the references to other people.

Where access is refused, the data subject may appeal to the courts or the Data Protection Commissioner.

WSHA are required to keep a record of all access requests from staff members or tenants and should also notify the Corporate Services Manager who keeps a central record of requests. The record should detail the request, action taken and timescales.

For further advice with regards to specific circumstances, the Information Commissioner can be contacted via the Information Commissioners office website: www.ico.gov.uk

Subject access – issues particular to social services

A data subject can make a request through agents such as a solicitor or social worker although they may be asked for evidence that they are acting on behalf of the data subject.

In cases where data subjects are incapable of understanding or exercising their rights, then subject access requests may be made by parents or other persons who are legally able to act on behalf of the data subjects.

Subject access to joint records

Where joint records are held between two or more organisations, the relevant organisations are required to be registered with the Information Commissioner's Office separately as each is a data controller in its own right.

The data subject should not have to apply to both organisations for access to his/her records. Either organisation can provide access to the joint record provided that the subject is informed that the data is held jointly.

The term 'joint record' does not include records held separately by organisations that contain information provided by either organisation to the other. While information held in each organisation's separate records might be similar, they cannot be considered as joint records. Parties to such exchanges are data controllers in their own right. In such cases data subjects requiring access must make separate applications to each controller.

Third Party Data

A person does not have the right to know what is recorded about someone else. So, for example, where there are files on an entire family and a request is recorded for access to one of these family files one member of the family is not entitled to see information about another member of the family without that person's consent.

In circumstances where the disclosure of the data requested is not possible without disclosing information about another person, normally the request need not be complied with unless the other person has given consent to the disclosure.

In such cases, efforts must be made to provide as much of the information sought as can be disclosed without revealing the identity of a third party, whether by omission of names or other identifying particulars. There may be circumstances to comply without consent. This includes the disclosure of identifiable details about a third party source.

When deciding what is reasonable to disclose when information includes details on a third party it is necessary to consider:

- Any duty of confidentiality owed to that third party
- Steps taken to get consent for the disclosure from the third party
- Whether the third party is capable of giving consent
- Any express refusal of consent by the third party

Requests for access to the records of a deceased person

The Data Protection Act applies only to data about living persons. Therefore data held on the deceased is not considered personal data as defined by the Act.

Even though the Data Protection Act does not apply, there may still be issues of confidentiality surrounding the rights of others to access records about the deceased.

Advice should be sought from the Information Commissioners Office where necessary.

Access can be refused if an identical or similar request from the same individual has previously been complied with, unless a reasonable interval has elapsed between compliance with the first and receipt of the subsequent request. In deciding what amounts to a reasonable interval, the following factors should be considered:

- The nature of information
- The purpose for which the information is processed
- The frequency with which the information is altered

West of Scotland Housing Association does not have to respond unless sufficient details are provided to enable it to locate the information and satisfy itself as to the identity of the individual making the request.

Where WSHA decides to refuse access

Any notification of refusal to disclose personal data should be given as soon as practicable and in writing, even if the decision has also been given in person.

A record should be kept of the reason for the decision and this should be explained to the data subject.

If West of Scotland Housing Association decides not to disclose some or all of the personal information, the applicant must be told the reasons, whether this is due to exemption, inability to obtain consent of the third part or their refusal to consent. Any refusal of access should be authorised by the relevant Director.

Challenge to West of Scotland Housing Association's decision to refuse access or amend records

If disclosure is refused by West of Scotland Housing Association, the data subject may appeal against that refusal either to the Information Commissioner's Office or the courts. It is for the data subject to decide which appeal route to take.

The Court has the power to order disclosure for example, or to order correction or erasure or to confirm non-disclosure.

The Information Commissioner's Office may issue enforcement notices for breach of the Data Protection Act and its principles, but only if the Commissioner is satisfied that a contravention has taken or is taking place.

Information that the data subject considers to be inaccurate

If a person considers that West of Scotland Housing Association holds personal information that is inaccurate in any way, he/she can take the following action:

- Ask the data controller to correct the data
- Approach the Commissioner if he/she considers the controller has not done so
- Apply to the courts for an order requiring the data controller to rectify, block, erase or destroy the data

The data controller may be required to correct data judged by the Information Commissioner's Office or courts to be inaccurate. The data controller may also be required to inform other organisations of the correction where necessary.

The data subject may also be entitled to compensation for any damage suffered as a result of the use of inaccurate data. "Inaccurate" means incorrect or misleading as to any matter of fact.

An opinion need not be corrected or removed, unless it appears to have been based on an inaccurate fact.

If West of Scotland Housing Association does not agree that the information is inaccurate it should note in the record that the subject regards the information as inaccurate.

Requests for data to be corrected should be dealt with promptly to avoid court action or intervention by the Commissioner. West of Scotland Housing Association will send a copy of the corrected data to the subject. The data subject should be notified within 21 days of action taken.

9 Protective Marking

Protective markings will be applied to any papers which are confidential. Protective markings should be applied using either a header, footer or a watermark – using these procedures will ensure the protective marking is applied to each page.

Protective Markings should be applied to documents where if the information from the document was compromised it would:

- Release private information about a staff member or tenant
- Cause unnecessary distress to staff members or tenants
- Would have an impact on the operations of the business
- Could adversely affect the Associations reputation
- Impede effective communication with our tenants

Papers which are marked confidential should be treated as such by all staff and should be shared with internal colleagues only on a need to know basis. Confidential papers should not be shared externally and only where permission is given (i.e committee members).

10 Electronic Data and Information

The principles for the management of electronic records are the same as those for the management of manual records. All data management standards detailed in section 3 apply to electronic records.

Effective electronic record keeping requires:

- A clear understanding of the nature of electronic records;
- The establishment and maintenance of a structure of folders to reflect logical groupings of records
- The secure maintenance of the integrity of electronic records e.g. password protected systems and access levels
- The accessibility and use of electronic records for as long as required (which may include their migration across systems)
- The application of appropriate disposal procedures, including procedures for archiving
- The ability to cross reference electronic records to their paper counterparts in a mixed environment. This is particular important in relation to Tenant and staff records.

Smart Phones

As e-mails sent or received can often contain personal information about an individual or other information deemed private and confidential, it is essential that all Smart Phones are password protected and that only the user has the password.

Scanning

As all of our photocopiers now have scanning facilities, scanning documents and e-mailing them is an effective way of sending information externally and reducing postage costs and paper usage.

Links

As we have the internal facility to do so we should send links to documents where possible rather than send them as attachments by email.

Faxing

Do not send personal information by fax, use the scanning facilities wherever possible. If there is no other option, ensure that you contact the person that you are faxing and advise them that you are sending the fax and ask them to stand by the fax machine to retrieve the document and phone you to confirm that they have received it. However, this should be avoided if possible.

11 Storage of Data

All data and information should be stored appropriately and the following should apply to both electronic and hard data and information:

- Clear and logical filing systems and structures should be in place to store information to assist with the retrieval of information, both electronic and paper based information.

- Paper based data and information should be stored in a clean, dry area in order to prevent any damage to files**.**

- Personal data and information regarding an individual should be stored in a locked filing cabinet. Access levels should be on a need to know basis and should be restricted appropriately.

- Information stored should be reviewed on a regular basis to ensure that it is up to date, accurate and still relevant for the purpose it is required for. We should not be keeping information that is incorrect, out of date or that we no longer require.

- Where possible, only current data and information that is in use should be stored in the office or electronic folders. All other paper based data and information should be archived either externally or in another area of the office e.g. locked archiving cupboard. Electronic data and information not in use should be stored in an archive facility on their PC. This ensures that staff are not dealing with vast quantities of information and can easily access current information. In relation to paper based information it ensures that office spaces are kept tidy.

- All staff should ensure that paper based data and information is filed on a regular basis and that personal data and information regarding an individual is stored securely and is never left on desks or in filing trays unless in a locked office that has limited access.

- If there is a combination of electronic and paper based data stored regarding an individual, ensure that the information is cross referenced to make a complete file to ensure that two separate differing records are not being kept.

12 Carrying Data outwith office bases

There may be times, where staff and volunteers are required to carry personal data outwith the office. This information should be kept to a minimum and should be carried electronically wherever possible. Hard copy information should only be carried if there is no other option.

In these cases the following should apply in relation to hard copy information:

- Information should only be taken out of the office if there is a clear purpose for the information as this should be limited as far as possible.
- The data and information should be anonymised as far as possible to ensure that is difficult to identify the individual.
- The information should be stored in a secure bag
- Staff and volunteers should be aware of their responsibilities relating to the security of the data and information they are carrying.

In relation to electronic information stored on a pen drive or laptop/netbook, the following should apply:

- As above the information should necessary and relevant and limited as far as possible
- As above the information should be anonymised as far as possible
- Any pen drives or laptops should be encrypted and password protected

The staff member should be aware that is their responsibility to keep that data and information safe and secure and take all reasonable precautions to ensure that information is not lost or stolen.

13 Retention Timescales

As mentioned previously, it is essential that we do not keep data and information that we are not required to keep. As this is the case, we have a retention schedule in place which should be followed by all staff and data and information should not be kept beyond these timescales – Appendix A.

When archiving your data and information, both paper based and electronic, you should detail on the box or file when the information should be destroyed in line with the retention timelines. Please note that these retention timescales also apply to information that is held on databases.

Retention of General Office Files
Whilst there is no specific legislation in connection with general office files such as general correspondence, minutes of internal meetings etc, West of Scotland Housing Association recommends that general files should kept in the office for one year and thereafter should be archived for no longer than 2 years.

Unless a record of signatures is required, the majority of general office information should be held electronically rather than by hard copy. This will avoid any unnecessary storage. Please ensure that you have adequate back up systems in place for the retention of electronic files.

As per section 12, CCTV records should be kept for no longer that 7 days unless the recording is being used in an investigation. Where this is the case it is suggested that recordings are held for no longer than four years.

The timescales will also ensure that data and information is manageable and can be stored and accessed effectively.

Considerations when deciding on retention periods

West of Scotland Housing Association staff should consider the following questions when deciding how long to retain a record before final disposition:

- Is the record still required for the day-to-day running of the association?
- Is it required for legal purposes (e.g. contracts)?
- Does any legislation or official regulation govern how long it must be kept?
- Is it likely to be of ongoing or recurrent public interest?

Retaining Records for Permanent Preservation

Records are designated as “archival” for many reasons, the main ones being that:

- they are still essential to the association
- they document the Associations policies, structures and processes so that its activities may be accountable to the present generation and understood by future generations.

In general, this means keeping records which provide evidence of the following matters**:**
- top-level decision making and policy formulation within the organisation
- policy making within the major functions of the organisation
- important or high profile aspects of the interactions between the organisation and individuals, businesses, civic institutions, and the environment

- principal administrative processes of the organisation structure and remit of the organisation, and any major changes to these.

14 Archiving Guidance and Procedures

As per section 9, Storage of Information, only current data and information that is in use should be kept in office files. This would usually be information relating to that calendar year or financial year for financial paperwork. Where possible these types of documents should be scanned to documotive as soon as possible.

All other information should be electronically archived. Where possible data and information should be archived electronically in order to save space and in some case to save money where external storage would be required. Archive data can be stored electronically in bulk through an agreement we have set up with a document management company. Files can be scanned and indexed in large quantities and we can receive data back on disks which can be moved to documotive.

All departments should review the data and information they hold on a regular basis. When archiving information staff should include the following:

- Any information that is over a year old should be electronically archived as per the retention schedule.
- Any information that is not required should be destroyed as per the retention schedule.
- Any information that is archived and due to be destroyed as per the retention schedule.

When archiving data and information, electronically or hard copies, the following should be applied:

- The data and information should be stored in a tidy and logical system.
- The archive box or electronic file should be labelled with the following information:
    - What is the data and information is e.g. Invoices,
    - The date that relates to the information e.g. 2010/2011 or September to November 2010
    - When the data and information should be destroyed
    - File/box number
- All archiving should be stored in a secure safe place lockable room or cupboard and there should be limited access.

15 Disposal Arrangements

It is essential that the disposal of records is undertaken in accordance with these policies and procedures.

All paper based records containing personal information should be shredded or disposed of through confidential waste systems.

All electronic records containing personal information should be deleted completely from the hard drive.

Records which are not selected for permanent preservation and which have reached the end of their administrative shelf life should be destroyed in as secure a manner as is necessary for the level of confidentiality or security markings they bear.

16 CCTV Systems

CCTV and other systems which capture images of identifiable individuals are also covered by the DPA.

Before deciding to install or to continue using a CCTV system it is important to conduct an impact assessment to determine if CCTV is justified and how it should be operated.

Issues to consider in the impact assessment include:

- Who will be using the CCTV images? Who will take legal responsibility under the DPA?
- What is the purpose for using CCTV? What problems is it meant to address?
- What benefits are to be gained from its use?
- Are images of identifiable individuals required?
- Will the system remain suitable in the future?
- What future demands may arise for wider use of images and how will these be addressed?
- What are the views of those who will be under surveillance?
- What can be done to minimise intrusion for those who will be monitored?

It is essential that appropriate camera equipment and locations are selected. Image capture should be restricted to ensure that cameras do not view areas that are not of interest and are not intended to be the subject of surveillance, such as individuals' private property.

Cameras must be sited and the system must have the necessary technical specification to ensure that images are of the appropriate quality.

A regular maintenance regime must be set up to ensure that the system continues to produce high quality images.

Regular checks must be carried out to ensure that the date and time stamp recorded on the images is accurate.

Recorded material must be stored securely and in a way that prevents damage to the image.

Recorded images should be viewed in a restricted area, such as a designated secure office.

Disclosure of images from the CCTV system should be controlled. Consideration should be given as to whether a request for disclosure is genuine and if there is any risk to other people involved.

The DPA does not prescribe any specific minimum or maximum retention periods for CCTV systems or footage, but images should not be kept for longer than is necessary. The timeframe for keeping images will be set on your equipment.

On occasion it may be necessary to keep images for a longer period, for example where they are being used by a law enforcement body investigating a crime. It is suggested that such footage is held for four years, in line with retention periods for general files.

CCTV signs must be displayed in order to let people know that they are in an area where CCTV surveillance is being carried out.

A CCTV code of practice is available from the Information Commissioner's Office website: www.ico.gov.uk

Glossary of Terms

Agent
Means a person authorised expressly by the data subject to act on his or her behalf.

Case Record
Means all the records held by West of Scotland Housing Association about a person for whom they have provided or are providing services.

Data
Means information which:

- is being processed by means of equipment operating automatically in response to instructions given for that purpose;
- is recorded with the intention that it should be processed by means of such equipment;
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
- does not fall within (a), (b) or (c) above but forms part of an accessible record.

Data Controller
Means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be, processed.

Data Processor
In relation to personal data, means any person (other than an employee of the Data Controller) who processes the data on behalf of the data controller.

Data Subject
Means an individual who is the subject of personal data.

DPA
Means the Data Protection Act, 1998.

Health Professional
Means:
(a) a registered medical practitioner
(b) a registered dentist as defined by section 53(1) of the Dentists Act, 1984,
(c) a registered optician as defined by section 36(1) of the Opticians Act, 1989
(d) a registered pharmaceutical chemist as defined by section 24(1) of the Pharmacy Act, 1954
(e) a registered nurse, midwife or health visitor
(f) a registered osteopath as defined by section 41 of the Osteopaths Act, 1993
(g) a registered chiropractor as defined by section 43 of the Chiropractors Act, 1994
(h) any person who is registered as a member of a profession to which the Professions Supplementary to Medicines Act, 1960, for the time being extends
(i) a clinical psychologist, child psychotherapist or speech therapist
(j) a music therapist employed by a health service body
(k) a scientist employed by such a body as head of a department.*(Section 69)*

Obtaining or Recording
In relation to personal data, includes obtaining or recording the information to be contained in the data.

Personal Data
Means data which relate to a living individual who can be identified:
(a) from those data, or
(b) from those data and other information which is in the possession or, or likely to come into the possession of, the data controller, and 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.

Processing
In relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:
(a) organisation, adaptation or alteration of the information or data
(b) retrieval, consultation or use of the information or data
(c) disclosure of the information or data by transmission, dissemination or otherwise making available; or
(d) alignment, combination, blocking, erasure, or destruction of the information or data.

Recipient
Means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular enquiry by or on behalf of that person made in the exercise of any power conferred by law.

Relevant Filing System
Means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals, or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Sensitive Personal Data
Means personal data consisting of information as to:
(a) the racial or ethnic origin of the data subject
(b) his political opinions
(c) his religious beliefs or other beliefs of a similar nature
(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992
(e) his physical or mental health or condition
(f) his sexual life
(g) the commission or alleged commission by him of any offence
(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Third Party
In relation to personal data, means any person other than:
(a) the data subject
(b) the data controller

(c) any data processor or other person authorised to process data for the data controller or processor.

Using or Disclosing
In relation to personal data, includes using or disclosing the information contained in the data.

List of Sources

- Calderdale Council – Protecting Data & Recording with Care
- Public Records Office (www.pro.gov.uk) – Records Management Standards
- Freedom of Information (Scotland Act) 2002
- Scottish Information Commissioner – Code of Practice on Records Management
- Department for Constitutional Affairs (www.dca.gov.uk)
- Information Commissioner (www.informationcommissioner.gov.uk)
    - Small Business Guidelines
    - The Employment Practice DP Code
    - Use & Disclosure of Health Data
    - DPA – Subject Access – A Guide for Data Subjects
    - CCTV code of practice, revised edition 2008
    - Getting it right – a brief guide to data protection for small businesses
    - A quick 'how to comply' checklist
    - Data Protection Good Practice Note – Checklist for handling requests for personal information (subject access requests)
- Data Protection Act 1998
- DPA 1998 – Compliance Advice – Subject Access - Right of Access to Social Services Records
- DPA 1998 – Compliance Advice – Subject Access & Health Records
- Health Records Act 1998
- Lord Chancellor's Code of Practice on the Management of Records
- National Keeper of the Records of Scotland
- National Housing Federation

Appendix A – Retention Schedule (Source – National Housing Federation)

1. Governance Documents				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Certificate of Incorporation	N/A	N/A	Permanently	Implied by CA, Sec.15.
Certificate of change of company name	N/A	N/A	Permanently	Implied by CA, Sec.80.
Memorandum and articles of association (original)	N/A	N/A	Permanently	Best practice.
Articles of association (current)	Permanently	CA	Permanently	Best practice.
Governance Documentation	N/A	N/A	Permanently	Required for charitable status.
Constitution, Aims and Objectives	N/A	N/A	Permanently	Required for charitable status.
Confirmation letter of charitable registration	N/A	N/A	Permanently	Best practice.
HMRC confirmation of charitable status	N/A	N/A	Permanently	Best practice
Registration documentation (I & P Societies)	Permanently	IPSA	Permanently	Best practice.
Certificate of registration with the housing regulator	N/A	N/A	Permanently	Best practice.

Board member documents – apt letters, SLAs, bank details etc	N/A	N/A	6 years after board membership ceases though some details should be destroyed when membership ceases eg bank details etc	DPA 1998 5th principle CA 2006 recommendation for docs post termination of directorship
2. Meetings (incl AGMs)				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Notices of meetings	N/A	N/A	6 years	In case of challenge to validity of meeting or
Permanently	CA	Permanently		Signed originals must be kept.
Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
resolutions. Board and committee minutes (companies)				
Board resolutions (companies)	Permanently	CA	Permanently	Signed originals must be kept.
Minutes and resolutions of trustees (charities)	N/A	N/A	Permanently	Charity Commission requirement CC48
3. Registrations and Statutory Returns:				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Annual returns to the regulator	N/A	N/A	5years	Best practice.
Audited company returns and financial statements (including I	N/A	N/A	Permanently	Best practice.

& P Societies' Annual Returns to Registrar of Friendly Societies)				
Declarations of interest	N/A	N/A	6 years	Limitation for legal proceedings.
Register of directors and secretaries	Permanently	CA	Permanently	
Register of Shareholding members	Permanently	CA	Permanently	Records may be removed from register 20 years after membership ceases.
Register of seals	N/A	N/A	Permanently	Best practice.
Register of share certificates	N/A	N/A	Permanently	Best practice.
List of members (I & P Societies)	N/A	N/A	Permanently	Required by Registrar of Friendly Societies.
Nursing home and residential care homes registration certificates	N/A	N/A	Permanently	Best practice.
Nursing home and residential care homes inspection reports	N/A	N/A	6 years following end of management	Limitation for legal proceedings. Reports are public documents.
4. Strategic Management				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Business plans & supporting documentation (e.g. organisation structures, aims, objectives, funding	N/A	N/A	5 years after plan completion	Best practice.

issues)				
5. Insurances				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Current and former policies	N/A	N/A	Permanently	Limitation can commence from knowledge of potential claim and not necessarily the cause of the claim. N.B. Housing Association Boards must annually reaffirm formally their continuation of the Voluntary Board Members Liability Policy (automatically provided via NHF membership). NCVO recommends 3 years after lapse.
Annual Insurance schedule	N/A	N/A	6 years	Best practice.
Claims and related correspondence	N/A	N/A	2 years after settlement	Zurich Municipal recommendation. NCVO
Indemnities and guarantees	N/A	N/A	6 years after expiry	Limitation for legal proceedings. 12 years

				if related to land.
Group health policies	N/A	N/A	12 years after cessation of benefit	Best practice
Employer's liability insurance certificate	N/A	N/A	40 Years	2008 regs removed requirement to retain for 40 years but need to be mindful of 'long tail' industrial disease claims etc.

6. Finance, Accounting & Tax Records

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Accounting records for Limited Company	3 years from the date made	CA Sec 388	6 years	TMA Sec.20. may require any documents relating to tax over 6 (plus) years.
Accounting records for I&P Society or Charity	N/A	N/A	6years	Required by Registrar of Friendly Societies and Charity Commissioner.
Balance sheets and supporting documents	N/A	N/A	6 to 10 years	Best practice. To relate to accounting records.
Loan account control reports	N/A	N/A	6years	Best practice.
Social Housing Grant documentation	N/A	N/A	Permanently	Best practice.
Signed copy of report and accounts	N/A	N/A	Permanently	Best practice.
Budgets and internal financial reports	N/A	N/A	2 years	Best practice.

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Tax returns and records	N/A	N/A	10 years	TMA Sec.20. may require any documents relating to tax over 6 (plus) years.
VAT records	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Orders and delivery notes	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Copy invoices	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Credit and debit notes	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Cash records & till rolls	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Journal transfer documents	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
Creditors, debtors & cash income control accounts	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.
VAT related correspondence	6 years	VATA	6 years	Customs & Excise requirement for VAT registered bodies.

7. Other Banking Records (including Giro)				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Cheques	N/A	N/A	6 years	Limitation for legal proceedings.
Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Paying in counterfoils	N/A	N/A	6 years	Limitation for legal proceedings.
Bank statements and reconciliations	3 years from the end of the financial year the transactions were made	CA	6 years	Limitation for legal proceedings.
Instructions to bank	N/A	N/A	6 years	Limitation for legal proceedings.
8. Contracts and Agreements:				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Contracts under seal and/or executed as deeds	N/A	N/A	12 years after completion (including any defects liability period)	Limitation for legal proceedings.
Contracts for the supply of goods or services, including professional services	N/A	N/A	6 years after completion (including any defects liability period)	Limitation for legal proceedings (12 years if related to land).
Documentation relating to small one-off purchases of goods and services, where there is no	N/A	N/A	3 years	Best practice. Suggested limit: goods or services costing up to £10,000.

continuing maintenance or similar requirement				
Loan agreements	N/A	N/A	12 years after last payment	Best practice.
Licensing agreements	N/A	N/A	6 years after expiry	Limitation for legal proceedings.
Rental and hire purchase agreements	N/A	N/A	6 years after expiry	Limitation for legal proceedings.
Indemnities and guarantees	N/A	N/A	6 years after expiry	Limitation for legal proceedings.
Documents relating to successful tender	N/A	N/A	6 years after end of contract	Best practice.
Documents relating to unsuccessful tenders	N/A	N/A	2 years after notification	Best practice.
Forms of tender	N/A	N/A	6 years	Best practice.

9. Charitable Donations

Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Deeds of covenant	6 years after last payment	TMA	12 years after last payment	Limitation for legal proceedings if related to land.
Index of donations granted	N/A	N/A	6 years	Best practice.
Account documentation	3 years	CA	6 years	Best practice.

10. Application and Tenancy Records:				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Applications for accommodation	N/A	N/A	6 years after offer accepted	Best practice.
Continuous Recording of lettings and sales (CORE) data record form	N/A	N/A	None	Best practice in DPA compliance requires form to be destroyed immediately statistics have been recorded.
Housing Benefit notifications	N/A	N/A	2 years	Recommendation of Institute of Rent Officers (now merged with CIoH).
Rent statements	N/A	N/A	2 years	Best practice.
Tenants' tenancy Files, including rent payment records, and details of any complaints and harassment cases	N/A	N/A	In general, for the length of the tenancy up to 6 years post tenancy. There may be occasion to weed very old, but still current, files.	Limitations Act 1980 and Best practice with DPA compliance 5th principle. For rent payment details, best practice suggests live system holds 2 years records plus current year.
Former tenants' Tenancy Agreements, and details of their leaving	N/A	N/A	6 years	Best practice with DPA compliance 5th principle
Care plans for children and related documents	75 years	Ch A	Permanently	Some documents may be transferred to subsequent caring

				agency.
Care plans for adults and related documents	N/A	N/A	Permanently	May be subject to DPA. Some documents may be transferred to subsequent caring agency.
Documentation, correspondence and information provided by other agencies relating to special needs of current tenants	N/A	N/A	While tenancy continues	Information held on 'need to know' basis. Medical and Social Services records liable to be confidential. To be returned or passed to subsequent agency at end of tenancy, or destroyed.
Records relating to offenders, ex-offenders and persons subject to cautions	N/A	N/A	While tenancy continues	Information held on 'need to know' basis. Police sourced records may be confidential. To
11. Property Records				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Rent registrations (superseded)	N/A	N/A	6 years	6 years if it has been superseded by a subsequent registration.

Rent Registration (not superseded)	N/A	N/A	Permanently	When no new fair rent has been registered (for example because there is no longer a Rent Act tenant in the property) the maximum recoverable rent will be applicable if a Rent Act tenant is ever moved into the property.
Fair rent documentation	N/A	N/A	6years	Rent Officer recommendation.
Leases and deeds of ownership	N/A	N/A	While owned Deeds of title –permanently or until property disposed of. Leases – Fifteen years after expiry [from NCVO]	Best practice.
Copy of former leases	N/A	N/A	12 years after settlement of all issues	Limitation for legal action relating to land or contracts under seal.
Wayleaves, licences and easements	N/A	N/A	12 years after rights given or received cease	Limitation for legal action relating to land or contracts under seal.
Abstracts of title	N/A	N/A	12 years after interest	Limitation for legal action
Planning and building control permissions	N/A	N/A	12 years after interest ceases	Limitation for legal action relating to land or contracts under

				seal.
Searches	N/A	N/A	12 years after interest ceases	Limitation for legal action relating to land or contracts under seal.
Property maintenance records	N/A	N/A	6 years	Limitation for legal action.
Reports and professional opinions	N/A	N/A	6 years	Limitation for legal action.
Development documentation	N/A	N/A	12 years after settlement of all issues	Limitation for legal action relating to land or contracts under seal.
Invoices	6 years	VATA	12 years	Limitation for legal action relating to land or contracts under seal.
VAT documentation	See Finance, Accounting & Tax Records section	See Finance, Accounting & Tax Records section	See Finance, Accounting & Tax Records section	See Finance, Accounting & Tax Records section
Insurance	See Insurances section	See Insurances section	See Insurances section	See section on insurance.
12. Vehicles				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Mileage records	N/A	N/A	2 years after disposal	Best practice.
Maintenance records, MOT tests	N/A	N/A	2 years after disposal	Best practice.
Copy registrations	N/A	N/A	2 years after disposal	Best practice.

13. Capital Assets				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Capital Assets	N/A		Date of purchase to at least 6 years after date sold, transferred or disposed of.	
Fixed Asset Register	CA Charities Act		Permanently	
14. Employees: Tax and Social Security				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Record of taxable payments	6 years	TMA	6 years	Inland Revenue require retention of each payment for 3 years.
Record of tax deducted or refunded	6 years	TMA	6 years	Inland Revenue require retention of each payment for 3 years.
Record of earnings on which standard National Insurance Contributions payable	6 years	TMA	6 years	Inland Revenue require retention of each payment for 3 years.
Record of employer's and employee's National Insurance Contributions	6 years	TMA	6 years	Inland Revenue require retention of each payment for 3 years.
NIC contracted-out arrangements	6 years	TMA	6 years	

Copies of notices to employee (e.g. P45, P60)	6 years plus current year	TMA	6 years plus current year	
Inland Revenue notice of code changes, pay & tax details	6 years	TMA	6 years	
Expense claims	N/A	N/A	6 years after audit	Best practice.
Record of sickness payments	3 years following year to which they relate	SSPR	6 years	Inland Revenue require retention of each payment for 3 years.
Record of maternity payments	3 years following year to which they relate	SMPR	6 years	Inland Revenue require retention of each payment for 3 years.
Income tax PAYE and NI returns	3 years following year to which they relate	IT(E)R	6 years	Best practice.
Redundancy details and record of payments & refunds	N/A	N/A	12 years	Institute of Personnel and Development (IPD) recommendation.
Inland Revenue approvals	N/A	N/A	Permanently	IPD recommendation
Annual earnings summary	N/A	N/A	12 years	Best practice.
15. Employees: Pension Schemes				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Actuarial valuation reports	N/A	N/A	Permanently	IPD recommendation.
Detailed returns of	N/A	N/A	Permanently	Best practice.

pension fund contributions				
Annual reconciliations of fund contributions	N/A	N/A	Permanently	Best practice.
Money purchase details	N/A	N/A	6 years after transfer or value taken	IPD recommendation.
Qualifying service details	N/A	N/A	6 years after transfer or value taken	IPD recommendation.
Investment policies	N/A	N/A	12 years from end of benefits payable under policy	IPD recommendation.
Pensioner records	N/A	N/A	12 years after benefits cease	IPD recommendation.
Records relating to retirement benefits	6 years after year of retirement	RBS(IP)R	6 years after year of retirement	Statutory requirement.

16. Employees (Personnel Procedures):				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Terms and conditions of service, both general terms and conditions applicable to all staff, and specific terms and conditions applying to individuals	N/A	N/A	6 years after last date of currency	Limitation for legal proceedings.
Service contracts for directors (companies)	3 years	CA	6 years after directorship ceases	Best practice.
Remuneration package	N/A	N/A	6 years after last date of currency	Limitation for legal proceedings.
Document	Statutory Retention Period	Statutory Retention Source	Recommended Retention Period	Comments
Former employees' Personnel Files	N/A	N/A	6 years	IPD recommendation.
References to be provided for former employees	N/A	N/A	20 years or until former employee reaches age 65 (whichever comes first)	Best practice.
Training programmes	N/A	N/A	6 years after completion	Best practice.
Individual training records	N/A	N/A	6 years after employment ceases	IPD recommendation.
Short lists, interview notes and related	N/A	N/A	1 year	IPD recommendation.

application forms,				
Application forms of non-shortlisted candidates	Three months after notification	SDA & RRA	6 months	Recommendation of Commission for Racial Equality and Equal Opportunities Commission. LA – 1 year limitation for defamations
CRB (Now DBS) clearance documentation	Date of clearance + up to a maximum of six months		Date of clearance + up to a maximum of six months	DBS check code of practice (Home office)
Time cards	N/A	N/A	2 years after audit	IPD recommendation.
Trade union agreements	N/A	N/A	10 years after ceasing to be effective	IPD recommendation.
Trust deeds, rules and minutes (for joint employee/employer sports/social clubs, etc, set up under trust)	N/A	N/A	Permanently	IPD recommendation.
Employer/employee committee minutes	N/A	N/A	Permanently	IPD recommendation.
Insurance claims	See Insurances section	See Insurances	See Insurances section	See Insurances section.
17. Employees: Health and Safety				
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
Health and Safety assessments	N/A	N/A	Permanently	IPD recommendation.
Medical records relating to control of	40 years	CAWR	40 years	

asbestos				
Health and Safety policy statements	N/A	N/A	Permanently	Good practice.
Records of consultations with safety representatives	N/A	N/A	Permanently	IPD recommendation.
Accident records, reports	3 years after date of settlement	RIDDOR	6 years after date of occurrence	Limitation for legal proceedings. DPA
Accident books	N/A	N/A	6 years after date of last entry	Limitation for legal proceedings.
Sickness records	Three years after the end of each tax year for Statutory Sick Pay purposes	SSP (general) regulations	6 years from end of sickness	Limitation for legal proceedings. NCVO recommends 3 years. However for industrial injuries not detectable within that period e.g. asbestos, the time period may be extended. Also for employees exposed to hazardous substances.
Health and safety statutory notices	N/A	N/A	6 years after compliance	Limitation for legal proceedings
Document	**Statutory Retention Period**	**Statutory Retention Source**	**Recommended Retention Period**	**Comments**
18.Technical and research				NCVO recommends 12-15 years after requirements have ended for both Records & reports and drawings & other data

19. ASB case files and associated documents				5 years or until end of legal action
20. Supporting people – subsidy claims / support plans / single assessments including supporting information				Duration of tenancy
21. Resident meeting minutes	N/A	N/A	One year	DPA

Appendix B – Destruction Authorisation

Box number	
Description of files to be destroyed	
Date from	
Date to	
Destruction date	
Senior Manager signature	
Date authorised	
Destroyed by	
Date destroyed	

Appendix C - Comparative Rights of Access under the Data Protection Act 1998 and Freedom of Information (Scotland) Act 2002

Issue	Data Protection	Freedom of Information
Who can apply for information?	Only the data subject, ie the living individual to whom particular data relates	Anyone anywhere
Who can a request be made to?	Any data controller within the public or private sectors	Any Scottish public authority
Can the organisation ask for proof of identity of the applicant?	Yes	No
How must an application be made?	In writing, including email	In writing, including email
What information can be requested?	All information relating to the data subject	Any recorded information held
Can a fee be charged?	Yes, generally up to £10	If organisation wishes to charge a fee, it must give the applicant a fees notice
How specific does the request have to be?	It must enable the organisation to locate the information requested.	It must enable the organisation to locate the information requested
Is there a limit on the amount of information that can be requested?	No	Yes, there is a limit to the amount of searching which an organisation must carry out to provide the information.
Must original documents be provided?	No	No
Can the applicant insist on having the information in a particular format?	No	No, the applicant cannot insist but can specify a preferred form
How long does the organisation have to respond?	Within 40 days of receiving a valid request and fee, if applicable	Within 20 working days

Appendix D - A quick 'how to comply' checklist

This short checklist will help you comply with the Data Protection Act (the Act). Being able to answer 'yes' to every question does not guarantee compliance, but it should mean that you are heading in the right direction. At the end is a list of guidance on particular areas where you may need more help as well as telephone helpline numbers.

- ☐ Do I really need this information about an individual?
- ☐ Do I know what I'm going to use it for?
- ☐ Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
- ☐ Am I satisfied the information is being held securely, whether it's on paper or on computer? And what about my website? Is it secure?
- ☐ Am I sure the personal information is accurate and up to date?
- ☐ Do I delete/destroy personal information as soon as I have no more need for it?
- ☐ Is access to personal information limited only to those with a strict need to know?
- ☐ If I want to put staff details on our website have I consulted with them about this?
- ☐ If I use CCTV, is it covered by the Act? If so, am I displaying notices telling people why I have CCTV? Are the cameras in the right place, or do they intrude on anyone's privacy?
- ☐ If I want to monitor staff, for example by checking their use of email, have I told them about this and explained why?
- ☐ Have I trained my staff in their duties and responsibilities under the Act, and are they putting them into practice?
- ☐ If I'm asked to pass on personal information, am I and my staff clear when the Act allows me to do so?
- ☐ Would I know what to do if one of my employees or individual customers asks for a copy of information I hold about them?
- ☐ Do I have a policy for dealing with data protection issues?
- ☐ Do I need to notify the Information Commissioner? If I have already notified, is my notification up to date, or does it need removing or amending?

For more help or advice on any of this, you can contact the Information Commissioner's Data Protection Helpline on 08456 30 60 60 (Lo-call rate) or 01625 545745 (National rate), or email using the online enquiry form on our website.