BUIDHEANN TIGHEADAS LOCH AILLSE AGUS AN EILEIN SGITHEANAICH
LOCHALSH AND SKYE HOUSING ASSOCIATION

Data Protection Policy and Procedures

Service: Corporate	Date	Staff Member
Version Number: 1		
Approved by: Management Committee	10/02/2014	N/A
Effective From:	10/02/2014	N/A
Next Review Date:	02/2019	CE
Revision Number:		
Revision Date:		
Posted on Intranet:		
Posted on Website:		
Publicity Material issued:		
Handbook(s) updated:		
Document Register updated:		
Previous Version archived:		
SSHC: Charter Standards and Outcomes:	N/A	

Scottish Social Housing Charter Relevant Standards and Outcomes

STANDARD	OUTCOME
N/A	

Contents

General Information

Lochalsh and Skye Housing Association is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 1998. The Association processes information about its staff, tenants and other individuals it has dealings with for a range of administrative purposes (e.g. to recruit and pay staff and comply with legal obligations to funding bodies and government). In order to comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

All "processing" of personal data (includes collection, holding, retention, destruction and use of personal data) are governed by the Data Protection Act 1998. The Act applies to all personal data - whether they are held on a computer or similar automatic system or whether they are held as part of a manual file. Personal data is defined as information relating to an identifiable living individual and can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Under the 1998 Act, all organisations that process personal information are required to notify the Information Commissioner's Office. The Association's Notification describes the various types of processing of personal information and defines the persons or bodies to which the information may be disclosed. Full details of the Association's notification can be found at http://www.informationcommissioner.gov.uk/ - the registration number is Z6024339.

It is an offence to process personal data except in strict accordance with the eight principles of data protection and the rights of data subjects. Further information on the Data Protection Act can be found at http://www.informationcommissioner.gov.uk/.

Failure to comply with the Data Protection Act could result in the prosecution not only of the Association but also of the individual concerned.

Data subjects (that is persons about whom such data is held) may also sue for compensation for damage and any associated distress suffered as a result of:

- loss or unauthorised destruction of data
- unauthorised disclosure of, or access obtained to, data
- inaccurate data - i.e. data which is incorrect or misleading

It follows, therefore, that all staff who are concerned with, or have access to, such data have an obligation to ensure that they are processed according to the eight principles of data protection and the rights of data subjects. This means, among other things, that staff must treat all data carefully and must not disclose personal data to unauthorised persons (this will often include parents or relatives of tenants or other data subjects).

You are specifically cautioned that Lochalsh and Skye Housing Association does not authorise any employee or agent of the Association to hold or process any personal

data on its behalf except as stated in the Association's Notification. Users of personal data within or outwith the Association's Office (e.g. pc at home or laptop) should consider the legal position before attempting to process personal data. This policy also applies to any subsidiary company of the Association.

In cases of doubt or difficulty staff should in the first instance contact the Association's Chief Executive.

REMEMBER - TREAT PERSONAL DATA WITH CARE. DON'T PASS ON PERSONAL INFORMATION TO UNAUTHORISED PERSONS

Eight Data Protection Principles

1. Data should be processed fairly and lawfully.
2. Data should be obtained for one or more specified lawful purposes.
3. Data shall be adequate, relevant and not excessive.
4. Data shall be accurate and where necessary kept up to date.
5. Data is not kept longer than is necessary for its purpose.
6. Data shall be processed in accordance with subject rights under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised/unlawful processing, loss, destruction, damage to personal data.
8. Data shall not be transferred outside EEA unless that country/territory ensures adequate level of protection for rights and freedoms of data subjects in relation to the processing of personal data.

Data Subject Rights

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about mechanics of automated decision taking process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by automated process
- To take action for compensation if they suffer damage by any contravention of the Act
- To take action to rectify, block, erase or destroy inaccurate data
- To request the Commissioner to assess whether any provision of the Act has been contravened

Section 1: Policy Statement

Lochalsh and Skye Housing Association is committed to a policy of protecting the rights and privacy of individuals (includes tenants, staff and others) in accordance with the Data Protection Act. The Association needs to process certain information about its staff, tenants and other individuals it has dealings with for administrative purposes (eg to recruit and pay staff, to administer tenancy agreements, to record progress, to collect fees, and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

The policy applies to all staff of the Association. Any breach of the Data Protection Act 1998 or the Association Data Protection Policy is considered to be an offence and in that event, Lochalsh and Skye Housing Association disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the Association, and who have access to personal information, will be expected to have read and comply with this policy. It is expected that departments/sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

Section 2: Background to the Data Protection Act 1998

The Data Protection Act 1998 enhances and broadens the scope of the Data Protection Act 1984. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent.

Section 3: Definitions (Data Protection Act 1998)

Personal Data

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, id number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject
Any living individual who is the subject of personal data held by an organisation.

Processing
Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data Accessing, altering, adding to, merging, deleting data Retrieval, consultation or use of data Disclosure or otherwise making available of data.

Third Party
Any individual/organisation other than the data subject, the data controller (Association) or its agents.

Relevant Filing System
Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System" in the Act. Personal data as defined, and covered, by the Act can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Tenant
The term “tenant” (meaning a tenant of the Association) is used throughout this policy. In most cases, “tenant” could be replaced with any other Data Subject who intends to use or is using a service administered by Lochalsh and Skye Housing Association.

Section 4: Responsibilities under the Data Protection Act

The Association as a corporate body is the data controller under the Act.
The Management Committee, Chief Executive, and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the Association.
Compliance with data protection legislation is the responsibility of all members of the Association who process personal information.
Members of the Association are responsible for ensuring that any personal data supplied to the Association are accurate and up-to-date.

Section 5: Notification

Notification is the responsibility of the Chief Executive. Details of the Association's notification are published on the Information Commissioner's website. Anyone who is, or intends, processing data for purposes not included in the Association's Notification should seek advice from the Chief Executive and the Notification updated accordingly.

Section 6: Data Protection Principles

All processing of personal data must be done in accordance with the eight data protection principles.

1. Personal data shall be processed fairly and lawfully.
   Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.
2. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.
   Data obtained for specified purposes must not be used for a purpose that differs from those.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.
   Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.
4. Personal data shall be accurate and, where necessary, kept up to date.
   Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the Association are accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify the Association of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Association to ensure that any notification regarding change of circumstances is noted and acted upon.
5. Personal data shall be kept only for as long as necessary.
   (see Section 12 on Retention and Disposal of Data)
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.
   (see Section 7 on Data Subjects Rights)
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.
   (see Section 9 on Security of Data)
8. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
   Data must not be transferred outside of the European Economic Area (EEA) – the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. Members of the Association should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

Section 7: Data Subject Rights

Data Subjects have the following rights regarding data processing, and the data that are recorded about them:

1. To make subject access requests regarding the nature of information held and to whom it has been disclosed.
2. To prevent processing likely to cause damage or distress.
3. To prevent processing for purposes of direct marketing.
4. To be informed about mechanics of automated decision taking process that will significantly affect them.
5. Not to have significant decisions that will affect them taken solely by automated process.
6. To sue for compensation if they suffer damage by any contravention of the Act.
7. To take action to rectify, block, erase or destroy inaccurate data.
8. To request the Commissioner to assess whether any provision of the Act has been contravened.

Section 8: Consent

Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The Association understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances consent to process personal and sensitive data is obtained routinely by the Association (eg when a potential tenant signs an application form, a tenant signs a Tenancy Agreement or when a new member of staff signs a contract of employment). Any Association forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data are to be published on the Internet as such data can be accessed from all over the globe. Therefore, not gaining consent could contravene the eighth data protection principle.

If an individual does not consent to certain types of processing (eg direct marketing), appropriate action must be taken to ensure that the processing does not take place.

If any member of the Association is in any doubt about these matters, they should consult the Chief Executive.

Section 9: Security of Data

All staff are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party (see Section 11 on Disclosure of Data for more detail).

All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- in a lockable room with controlled access, or
- in a locked drawer or filing cabinet, or
- if computerised, password protected

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.

This policy also applies to staff who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff should take particular care when processing personal data at home or in other locations outside Morrison House.

Section 10: Rights of Access to Data

Members of the Association have the right to access any personal data which are held by the Association in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by the Association about that person.

Any individual who wishes to exercise this right should apply in writing to the Chief Executive. The Association reserves the right to charge a fee for data subject access requests (currently £10). Any such request be complied with within 40 days of receipt of the written request and, where appropriate, the fee. See Subject Access Request Procedure more detail. For information on responding to subject access requests see Appendix 1 of this policy.

In order to respond efficiently to subject access requests the Association needs to have in place appropriate records management practices.

Section 11: Disclosure of Data

The Association must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff and tenants should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of Association business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the Association concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

1. the individual has given their consent (eg a tenant/member of staff has consented to the Association corresponding with a named third party);
2. where the disclosure is in the legitimate interests of the Association (eg disclosure to staff - personal information can be disclosed to other Association employees if it is clear that those members of staff require the information to enable them to perform their jobs);
3. where the Association is legally obliged to disclose the data (eg Health and Safety returns, ethnic minority and disability monitoring);
4. where disclosure of data is required for the performance of a contract.

The Act permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security*;
- prevention or detection of crime including the apprehension or prosecution of offenders*;
- assessment or collection of tax duty*;
- discharge of regulatory functions (includes health, safety and welfare of persons at work)*;
- to prevent serious harm to a third party;
- to protect the vital interests of the individual, this refers to life and death situations.

* Requests must be supported by appropriate paperwork.

When members of staff receive enquiries as to whether a named individual is a member of the Association, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed above (ie consent not required), the member of staff should decline to comment. Even confirming whether or not an individual is a member of the Association may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request.

As an alternative to disclosing personal data, the Association may offer to do one of the following:

- pass a message to the data subject asking them to contact the enquirer;
- accept a sealed envelope/incoming email message and attempt to forward it to the data subject.

Please remember to inform the enquirer that such action will be taken conditionally: ie "if the person is a member of the Association" to avoid confirming their membership of, their presence in or their absence from the Association.

Further information regarding the disclosure of personal information can be found in Appendices V (tenant information) and VI (telephone protocol).

If in doubt, staff should seek advice from their Line Manager or the Chief Executive.

Section 12: Retention and Disposal of Data

The Association discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on current staff and tenants. However, once a member of staff or tenant has left the Association, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

Tenants

In general, electronic tenant records containing information about individual tenants are kept indefinitely and information would typically include name and address, date of entry and date of exit.

Departments should regularly review the personal files of individual tenants.

Staff

In general, electronic staff records containing information about individual members of staff are kept indefinitely and information would typically include name and address, positions held, leaving salary.

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. The Association may keep a record of names of individuals that have applied for, be short-listed, or interviewed, for posts indefinitely. This is to aid management of the recruitment process.

Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (eg, shredding, disposal as confidential waste, secure electronic deletion).

Section 13: Publication of Association Information

All members of the Association should note that the Association publishes a number of items that include personal data, and will continue to do so. These personal data are:

- Information published in the Associations Corporate Diary
- Names of all members of Association Committees
- Names and job titles of staff.
- Internal Telephone Directory.
- Information in publications (including photographs), annual reports, newsletters, etc.
- Staff information on the Association website (including photographs).

It is recognised that there might be occasions when a member of staff or a tenant requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals should be offered an opportunity to opt-out of the publication of the above (and other) data. In such instances, the Association should comply with the request and ensure that appropriate action is taken.

Section 14: Direct Marketing

Any department or section that uses personal data for direct marketing purposes must inform data subjects of this at the time of collection of the data. Individuals must be provided with the opportunity to object to the use of their data for direct marketing purposes (eg an opt-out box on a form).

Section 15: Academic Research

Personal data collected only for the purposes of academic research (includes work of staff and tenants) must be processed in compliance with the Data Protection Act 1998.

Researchers should note that personal data processed ONLY for research purposes receive certain exemptions (detailed below) from the Data Protection Act 1998 if:

1. the data are not processed to support measures or decisions with respect to particular individuals AND

2. if any data subjects are not caused substantial harm or distress by the processing of the data

If the above conditions are met, the following exemptions may be applied to data processed for research purposes only:

- personal data can be processed for purposes other than that for which they were originally obtained (exemption from Principle 2);
- personal data can be held indefinitely (exemption from Principle 5);
- personal data are exempt from data subject access rights where the data are processed for research purposes and the results are anonymised (exemption from part of Principle 6 relating to access to personal data).

Other than these three exceptions, the Data Protection Act applies in full. The obligations to obtain consent before using data, to collect only necessary and accurate data, and to hold data securely and confidentially must all still be complied with.

Notes to Researchers

Whilst the Act states that research may legitimately involve processing of personal data beyond the originally stated purposes (eg longitudinal studies), the Association hopes that, wherever possible, researchers will contact participants if it is intended to use data for purposes other than that for which they were originally collected.

For those departments which gather sensitive personal data (as defined by the Act, see Section 3 on Definitions), extra care should be taken to ensure that explicit consent is gained and that data are held securely and confidentially so as to avoid unlawful disclosure.

Publication

Researchers should ensure that the results of the research are anonymised when published and that no information is published that would allow individuals to be identified. Results of the research can be published on the web or otherwise sent outside the European Economic Area but if this includes any personal data, the specific consent of the data subject must, wherever possible, be obtained.

Review

This document will be reviewed by the Management Committee or Sub-Committee set up for that purpose in accordance with the requirements of the Association's Register of Policies and Procedures.

Section 16: Appendices

More detailed guidance on the following issues has been published by the Association:
Subject Access Request Procedure
Appendices

I(a) Procedure for Subject Access Requests
I(b): Handling Subject Access Requests
II: Tenant Records Management
III: Staff Records Management
IV: Disclosure of Tenant Information
V: Telephone Protocol for the Disclosure of Personal Information
VI: References
VII: Photographs to be used in Publicity/Promotional Material

I(a) Procedure for Subject Access Requests

Individuals wishing to access their personal information should submit a request in accordance with the following notes:

1. Make your request, in writing, to the Chief Executive.

2. The request should include details and provide documented evidence of who you are (e.g. driving licence, passport, birth certificate). You should also provide as much detail as possible regarding the information you wish to access (e.g. where and by whom information is believed to be held, specific details of information required etc).

3. You are not required to state WHY you wish to access the information: the details we require are merely those that will aid the efficient location and retrieval of information.

4. The Association adopts a general policy of openness in terms of allowing individuals access to their personal information and wherever possible we aim to waive the administration fee (permitted under the Data Protection Act 1998).

5. Once the Chief Executive receives a Subject Access Request, all efforts will be made to fully comply within 40 days. In any event, you will receive all the information that has been located and can be released within 40 days and an explanation for any information that cannot be provided at that time.

6. In accordance with the Data Protection Act 1998, the Association does not usually release information held about individuals without their consent. Therefore if information held about you also contains information related to a third party, the Association will make every effort to anonymise the information. If this is not possible, and the Association has been unable to secure the relevant consent, the Association may decide not to release the information.

I(b) Handling Subject Access Requests

These guidance notes cover the procedures for handling “Subject Access Requests” and should be read in conjunction with the Association's Data Protection Policy. This document is Appendix I(b) to the policy.

Section 1: General - What is a Subject Access Request?

The Data Protection Act 1998 gives individuals (data subjects) a number of rights including the right to access personal data that an organisation holds about them. This right of access extends to all information held on an individual and includes personnel files, tenant record files, databases, interview notes and emails referring to the individual. If an individual makes a request to view their information, it is known as a “Subject Access Request”. It is permissible for the Association to charge a fee of up to £10 for responding to Subject Access Requests (see Section 6 for more detail).

The Act stipulates that the data subject must:

- make the request in writing
- supply information to prove who they are (to eliminate risk of unauthorised disclosure)
- supply appropriate information to help the Association to locate the information they require.

Upon receipt of a request, the Association must provide:

- information on whether or not the personal data are processed
- a description of the data, purposes and recipients
- a copy of the data
- an explanation of any codes/jargon contained within the data.

The Association must respond to Subject Access Requests within 40 days.

For further information, see the Association procedure to be followed when submitting a Subject Access Request.

Section 2: Responding to "Simple" Requests

Whilst data subjects are entitled to request all the information that an organisation holds on them, experience shows that they are usually looking for something specific.

Therefore, the majority of requests received by the Association are likely to be from staff and tenants asking for copies of a specific document(s). These will usually be located from a single source - typically the house files - and will not involve the disclosure of information relating to a third party (see Section 4 for more detail). In such cases, Association policy is to be open and transparent and wherever possible to let the individual have a copy of the information with minimum fuss. Such requests should be handled directly by the relevant department or section and there should be no need to involve the Association's Chief Executive. When responding to such requests, take care to ensure that you do not inadvertently release third party information without their consent (see Section 4 for further detail). No fee should be charged (see Section 6 for more detail).

Section 3: Responding to "Complex" Requests

There may be some instances when a request for information is more complex and will need to involve the Association Chief Executive to ensure a co-ordinated response. It is hoped that such requests will be infrequent.

Examples of situations where more complex requests might arise include:

- request involves locating information from multiple sources
- request involves the release of contentious information
- request is one in a series of requests from the same individual
- request involves the release of third party data for which consent has been refused or cannot be obtained (see Section 4 for further information)
- the data subject does not want to ask for the information from the department that holds it.

In such cases, the request should be referred to the Association's Chief Executive who will ensure that a co-ordinated approach is adopted and will determine whether or not it is appropriate to charge a fee. When responding to Subject Access Requests, the Chief Executive will liaise with staff in the department/section as appropriate.

Section 4: Third Party Data

It will sometimes be the case that responding to a Subject Access Request will lead to incidental disclosure of details relating to some other third party (for example, a referee or another tenant). Such third party information should not be disclosed without first seeking the consent of the third party.

If consent cannot be obtained (eg the third party cannot be contacted) or is refused, then the Association needs to consider whether or not disclosure is reasonable, taking into account:

- any duty of confidentiality owed to the third party
- the steps taken to seek consent
- whether the third party is capable of giving consent
- any express refusal of consent

If you are unable to obtain consent, you are advised to contact the Chief Executive who will have to consider/balance the impact on the third party of the disclosure, and the impact on the data subject of the disclosure being withheld. Where third parties have been acting in an official capacity it may be argued that the duty of confidence is lower than is otherwise the case. However decisions will be made on a case by case basis.

If the Chief Executive decides that disclosure cannot be made, only that information which could identify the third party should be withheld (eg third party details are blanked out). Wherever possible, the Association will follow good practice by explaining to the data subject that some information has been withheld, and why.

Third parties who regularly supply information on tenants/staff in a professional capacity should be informed that anything they submit may become available to the data subject through a Subject Access Request. Departments are advised to seek consent to disclose at the collection stage (e.g. when requesting references) to avoid delay upon receipt of a Subject Access Request. Where professionals request that information supplied by then be kept confidential, they must supply details of the exceptional reasons for making the request. The Association will consider those reasons in order to decide whether they are valid.

Section 5: Records Management

The maintenance of appropriate records is extremely important in the event of a Subject Access Request. Knowing who keeps what and where is central to the effective and efficient retrieval of information.

The other important aspect of records management is ensuring that only appropriate information is retained. This will reduce the amount of information which must be disclosed (thereby saving time and administrative costs associating with locating and supplying the information) but will also avoid embarrassment and potential damage to the Association's reputation by ensuring that inappropriate information is not being retained on individuals.

All staff are advised:

- to be careful about what personal information they keep (including emails)
- to try to only record factual information
- where it is necessary to record an opinion about an individual, to make sure it is justified and wherever possible backed up with factual evidence
- NOT to record anything that they would not wish the data subject to see.

There are many long-term aims of rationalising the information held by the Association. It will certainly help us to respond effectively to Subject Access Requests. The fewer data sources the Association has, the easier it will be to search these on receipt of a Subject Access Request. Wherever possible, we should be aiming to manage data on a single central database. All staff are encouraged not to hold files on individual tenants or staff members, but to lodge any such information with "designated individuals". Personal data of departed staff and tenants should be

reclaimed from any remote sources and stored in a single location or on a single database, with appropriate security and back-up.

Section 6: Association Position on charging for Subject Access Requests

The Act permits organisations to charge up to £10 for responding to Subject Access Requests. However, this is unlikely to cover the costs of responding to requests, particularly when it involves locating information from numerous sources or where large volumes of information need to be photocopied and posted. There is no scope within the Act to charge more than £10 and wherever possible, the Association aims to waive this fee. Experience shows that this tends to limit requests to certain documents rather than an Association-wide search and therefore reduces the workload associated with Subject Access Requests. If the Association were to receive numerous requests from one individual, it may consider introducing the charge and is well within its rights to do so.

There may be other circumstances when a charge is made such as:

- the data is difficult to locate or is held in multiple locations
- there are large volumes of data to be supplied
- consent from several third parties is required

If you receive a request for which you feel a charge should be made, please contact the Chief Executive for advice in the first instance.

Section 7: Exemptions

There are certain situations where the Association may not be obliged to release information in response to a Subject Access Request.

Examples include:

- Data containing information relating to a third party for which consent to release the information cannot be obtained (see Section 4 for more detail)
- Management forecasts such as plans for redeployment, restructuring, promotions (if they would prejudice conduct of business/activity)
- Information relating to legal proceedings being taken by the Association against an individual.

Exemptions are an extremely complex part of the Act and must be treated with caution. If you think that an exemption might apply to a Subject Access Request received by your department, you should contact the Chief Executive in the first instance.

II Tenant Records Management

These guidance notes should be read in conjunction with the Association's Data Protection Policy.

The Data Protection Act 1998 gives individuals the right to access the information that an organisation holds on them. In order to comply with this part of the Act, organisations need to have in place effective means of extracting and retrieving information from a variety of sources.

Housing Services hold a great deal of information on their Tenants, usually in a variety of forms and locations. In order to comply with a subject access request, the Association will need to be able to locate and collate the information quickly. It is therefore vital that key personnel know what information is held and by whom. Ideally, all information relating to individual Tenants should be kept in the House files (paper or electronic) so that, in the event of a subject access request, the Association can be confident that all the information is easily accessible from a limited number of central sources. However, the Association recognises that this may not always be the case in practice. The Association should ensure that Tenant record files are as complete as possible but it is acknowledged that there may be some instances where designated individuals* need to retain information on Tenants which would not be appropriate for more general access.

The Chief Executive will be responsible for agreeing lists of designated individuals within the section who are likely to hold information on Tenants.

Information held on Tenants can be categorised in one of two ways:

i) “classified information” is information which a Tenant has requested be kept confidential between the Tenant and the designated individual to whom they disclose the information. Designated individuals should give Tenants the opportunity to define information as classified (when, for instance, unauthorised access/disclosure of the information concerned to other staff in the department poses a risk of damage/distress to the Tenant).
ii) “unclassified information” is all other information held on Tenants which will be available for general access by designated individuals.

The following guidelines should be followed:

1. Copies of unclassified information relating to an individual Tenant should be lodged in the House record file.
2. Designated individuals may retain copies of classified information without copying it to the House record file.
3. Designated individuals may retain duplicate copies of any documentation (whether electronic or paper), particularly if the information is consulted on a regular basis.
4. Members of staff, other than those responsible for the House record files and designated personnel, should not retain information (electronic or paper) about individual Tenants.

5. Information should only be retained in accordance with the suggested retention periods in the Association's Records Retention Schedule.
6. When a designated individual leaves the Association, they should pass all information to the member of staff responsible for House files, to be either destroyed (in accordance with the Association's records retention schedule), or filed in the House record file, or passed to a replacement designated individual.
7. Tenants should be informed of what information is being held about them, what it will be used for, where it will be stored, and to whom it might be disclosed. This will normally be achieved via Housing Application forms and other data collection forms.

If these guidelines are followed, personal information held on Tenants can be easily located from a limited number of sources and departments will be much better prepared to respond to subject access requests efficiently.

III Staff Records Management

The Data Protection Act 1998 gives individuals the right to access the information that an organisation holds on them. In order to comply with this part of the Act, organisations need to have in place effective means of extracting and retrieving information from a variety of sources.

The Association holds a great deal of information on its staff. In order to comply with a subject access request, the Association will need to be able to locate and collate the information quickly. All information relating to individual staff should be kept in the staff record files (paper or electronic) so that, in the event of a subject access request, the Association can be confident that all the information is easily accessible from a limited number of sources. However, the Association recognises that this may not always be the case in practice. It is acknowledged that there may be some instances where designated individuals* need to retain information on staff which would not be appropriate for more general access.

*The Chief Executive will be responsible for agreeing lists of designated individuals

The following guidelines should be followed:

1. Wherever possible, copies of documentation relating to an individual member of staff should be lodged in the staff record file(s) (paper or electronic).
2. Designated individuals are permitted to retain duplicate copies of any documentation (electronic or paper), particularly if the information is consulted on a regular basis.
3. Exceptionally, designated individuals may also keep documentation relating to sensitive information (e.g. relating to health or other problems) without copying the information to the staff record file. Designated individuals should only follow this practice when unauthorised access/disclosure of the information concerned to other staff poses a risk of damage/distress to the member of staff.
4. Members of staff, other than those responsible for the staff record files and designated personnel, should not retain information (electronic or paper) about individual members of staff.
5. The exception to this is email as it would be impractical for staff to pass all emails to a central source. However, all staff must be aware that in the event of a subject access request, they may be asked to search their email archives for all emails referring to the member of staff that has made the request. Therefore, staff are advised not to keep emails relating to other members of staff unless it is absolutely necessary. In writing emails referring to other members of staff, you are reminded that, in the event of a subject access request, that member of staff is entitled to receive copies of all emails which refer to them.
6. Information should only be retained in accordance with the suggested retention periods in the Association’s Records Retention Schedule.
7. Staff should be informed of what information is being held about them, what it will be used for, to whom it might be disclosed and whether or not it will stored staff record file.

If these guidelines are followed, personal information held on staff can be easily located from a limited number of sources and the Association will be much better prepared to respond to subject access requests efficiently.

IV Disclosure of Tenant Information

The Association must ensure that personal data held on Tenants are not disclosed to unauthorised third parties including family members, friends, government bodies and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on Tenants to third parties.

These guidance notes should be read in conjunction with the Association's Data Protection Policy, which includes a section on Disclosure of Data. This document is Appendix V to the Data Protection Policy.

Section

Section 1: General Information

Disclosing Personal Data

In accordance with Principle 1 of the Data Protection Act, personal data should only be disclosed if one of the conditions set out in Schedule 2 are met. The most likely conditions applicable to the disclosure of Tenant data to third parties are:

- the Tenant has given their consent
- the disclosure is in the legitimate interests of the Association or the third party to whom the information is being disclosed (except where this would prejudice the rights, freedoms or legitimate rights of the Tenant)
- statutory obligation of the Association (eg statistical returns)
- disclosure is required for performance of a contract (eg contract between Tenant, the Association and Contractor)

Disclosing Sensitive Personal Data

In accordance with Principle 1 of the Data Protection Act, sensitive personal data (racial or ethnic origin, political opinions, religious beliefs, trade union membership,

health, sex life, criminal convictions) should only be disclosed if one of the conditions set out in Schedule 2 (see above) AND one of the conditions set out in Schedule 3 are met. The most likely conditions (of Schedule 3) applicable to the disclosure of sensitive Tenant data to third parties are:

- the Tenant has given their explicit (ideally written) consent
- statutory obligation of the Association (eg equal opportunities monitoring)
- disclosure is in the vital interests of the Tenant (eg information relating to a medical condition may be disclosed in a life or death situation)

Disclosing Personal Data Overseas

In accordance with Principle 8 of the Data Protection Act, personal data should only be disclosed outside of the EEA (the EU Member States together with Iceland, Liechtenstein and Norway) if one of the conditions set out in Schedule 4 are met. The most likely conditions applicable to the disclosure of Tenant data to third parties overseas are:

- the Tenant has given their explicit (ideally written) consent
- disclosure is required for performance of a contract
- disclosure is necessary for the purpose of any legal proceedings
- Informing Tenants of Disclosures and Obtaining Consent

Tenants should be informed of predictable disclosures (such as confirmation of Tenant status, responding to a request for a reference) when they register with the Association. Some Tenants will choose to opt out of certain processing (including disclosures). This information should be recorded on the Association database and all staff should check a Tenant's record before releasing any information.

In less predictable situations (eg parent phoning for financial details) where the Tenant has not been previously informed of a possible disclosure, the Tenant should give their consent before any information is released.

The Association understands "consent" to mean that the Tenant has signified their agreement whilst being in a fit state of mind to do so and without pressure being exerted upon them. There must be some active communication between the parties, consent cannot be inferred from non-response to a communication. In most cases, verbal consent should be acceptable so long as proper security checks are made to ensure that the person giving the consent is the Tenant. For telephone consent, this will mean asking the subject to confirm several separate facts that should be privy only to them (Tenant identity number, date of birth etc). For sensitive data, explicit written consent of Tenants should be obtained unless an alternative legitimate basis for processing exists (see above).

There are certain exemptions (Section 29) from the requirement to inform Tenants of disclosures if the information is being released for the prevention or detection of crime AND if informing the Tenant of the disclosure would prejudice the enquiries. See Section 2 for further detail.

Requirement to Disclose?

Unless there is a legal or statutory obligation, you are advised not to disclose any personal information about Tenants without their consent. Please note that disclosure includes confirmation of a Tenant's residence with the Association. If you are in any doubt as to the legitimacy of a disclosure, then no disclosure should be made.

Method of Disclosure

Disclosures should not be made over the telephone. The minimum security option is to take a number and ring the enquirer back. However, it is strongly advised that all enquirers should be asked to submit their requests in writing (where appropriate on headed paper). Once you have checked whether or not the request is legitimate, you should, wherever possible, reply in writing.

Section 2: Disclosure to Work Colleagues

You should always think carefully before disclosing Tenants' personal information to work colleagues whether they be from within, or external to, your own department. Under the Data Protection Act, you should not disclose personal data to colleagues unless they have a legitimate interest in the data concerned. As there is no definition as to what a "legitimate interest" is, it will have to be a matter of judgement in each case. As a rule you should consider whether or not the information is necessary to allow your colleague to perform their job.

When sharing information with colleagues, you should consider the level of detail necessary to enable them to perform their job. So for instance, if you knew that a Tenant was going to be absent from their accommodation for a significant period of time, you may wish to notify colleagues in the department of this fact. However, it might not be appropriate for all colleagues to be made aware of the specific reasons (health or otherwise) resulting in the absence.

Section 3: Disclosure to Relatives/Guardians and Friends

The Association has no responsibility or obligation to disclose any personal information relating to Tenants to relatives, even if they are contributing to the rent or other fees.

All Tenants should be given the opportunity, both on their Tenancy Agreement and Housing Application Form to provide the name of a nominated individual to whom the Association may disclose personal information. You should always check a Tenant's record to see whether or not they have identified a nominated individual. You may come under pressure to discuss individual Tenants with parents/guardians or even friends. However, in these situations it is essential that you do not disclose personal data without the prior consent of the Tenant - it would be a breach of the Data Protection Act to do so. If the Tenant has identified a nominated individual (see above) they are understood to have given prior consent.

You are, of course, free to discuss procedures with parents (eg describing allocations procedures, advising on when rent should be paid by) but the specific circumstances of an individual Tenant cannot be discussed without the consent of that Tenant.

There may be occasional, exceptional circumstances (in which a Tenant’s life or health is threatened) in which the usual need to get consent before disclosing to parents/guardians may be waived. The Association holds details of Tenants' "next of kin" for such purposes.

Section 4: Confirmation of Tenant Status

Tenant status is regarded as personal data and therefore must be processed in accordance with the Data Protection Act, this includes protecting the information against unauthorised disclosure. By confirming whether or not an individual is (or has been) a Tenant of the Association could be a breach of the Act.

The Association receives enquiries regarding individuals' Tenant status on a regular basis. The nature of the third party requiring the information can range from future providers of rented housing genuinely trying to confirm details on a housing application form to estranged or abusive partners trying to trace an individual's whereabouts. Therefore, whenever faced with a request for confirmation of Tenant status, you should exercise caution before responding. The majority of requests will be from agencies with a genuine interest in the information. For this reason, Tenants are informed (on their application form) that, if requested, details of their Tenant status will be disclosed to certain named bodies. Tenants are given an opportunity to opt out of these disclosures and so you should always check the Tenant's record before responding. You should always employ appropriate security measures to check the identity of the enquirer and you should not disclose the information over the telephone. Wherever possible, ask the enquirer to put their request in writing, preferably on headed paper.

For other enquirers, where there is no statutory or other legal obligation for you to disclose information, you should not confirm or deny the Tenant status of an individual without their consent.

Section 5: Disclosure to Highland Council (includes Housing Benefit Administration)

Tenants are informed that details of their tenancy may be passed to the Highland Council on their Housing Application Form and are given an opportunity to object to such disclosures.

Where the Tenant is in receipt of Housing Benefit. You are advised to make the tenant aware that their acceptance of benefit will indicate consent for their details to be disclosed to Highland Council. Only relevant information should be released.

Section 6: Requests for Personal References

If you receive a request for a personal reference relating to a Tenant, you should ensure that

1. the information contained in the reference is FACTUALLY correct
2. where possible, keep the disclosure to a minimum
3. sensitive data (e.g. details of health) must not be disclosed without the explicit consent of the Tenant
4. where opinions about a person's suitability are disclosed, your comments are defensible and justifiable on reasonable grounds
5. if you are unable or unwilling to give a reference, such a refusal is communicated carefully, without, in effect, implying a negative reference and thus disclosing personal data
6. you do not disclose any information if asked to give an unsolicited reference (for a Tenant who has not, to your knowledge, cited your name as a referee)

The identity of the person requesting the reference should always be confirmed prior to disclosure. Requests for references should usually be made in writing on headed paper. If you receive an email request for a reference, you should be assured that it is a valid request. If it is from a known source or company domain, you should process the request but you may wish to reply in written format to a known postal address for the company/organisation. If the email domain is not familiar, you are advised to investigate further.

Telephone references are not usually recommended. However, they are acceptable if the Tenant has specifically asked you to provide a reference at short notice. As a minimum security measure it is recommended to ring the enquirer back to check that they are who they claim to be.

Tenants are informed, on the Tenancy Agreement that we will confirm Tenant status to future housing providers. Tenants are, of course, given the opportunity to opt out of this and if they do so, it will be recorded on their Tenant record. The Tenant Handbook also informs Tenants that we archive Tenant records after termination of the tenancy, in order to confirm requests from future housing providers, to provide references etc.

If a Tenant cites your name as a referee, it is understood that they are giving consent for you to disclose information (regardless of whether they have opted out on the Tenancy Agreement). If you are not aware that a Tenant has cited you as a referee, you should check the validity of the request.

Section 6: Disclosures to the Police and Legal Proceedings

Disclosures to the Police

Disclosures to the Police are NOT compulsory except in cases where the Association is served with a Court Order requiring information. However, Section 29 of the Data Protection Act 1998 does allow limited exemptions from the first Principle meaning that the Association may release information to the Police without the consent of Tenants in limited circumstances. Such disclosures should only be made if the Police confirm that they wish to contact a named individual about a specific criminal

investigation and where the Association believes that failure to release the information would prejudice the investigation. Staff must not release information to the Police over the telephone. The Police must inform the Association in writing. Most Police Forces will have their own request form which should always include a statement confirming that the information requested is required for the purposes covered in Section 29, a brief outline of the nature of the investigation, the Tenant's role in that investigation, and the signature of the investigating officer.

Legal Proceedings

Section 35(2) of the 1998 Act exempts data from the non-disclosure provisions (eg obtaining consent from Tenant) in cases where disclosure is necessary "for the purpose of, or in connection with, legal proceedings…..or for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights". In practice this means that the Association can disclose information regarding Tenants to its own solicitors when seeking proper legal advice about a case. However, for cases that do not directly involve the Association, information should only be disclosed if the relevant Tenant's permission can be obtained. If the information is vital to a case, a Court Order may be issued demanding the information. Section 35(1) specifically allows data controllers to disclose without consent from the data subject (Tenant) when confronted with a Court Order.

Section 7: Audit

Like all other Housing Associations, Lochalsh and Skye Housing Association appoints external and internal auditors who will see some Tenants' personal data during the course of their investigations. Tenants are made aware of this possibility when they sign the Tenancy Agreement and in the Tenant Handbook and therefore, in signing, give their consent for disclosure to auditors.

Section 8: Survey/Research Organisations

Survey/Research Organisations may approach you for a list of addresses or emails for Tenant so that they can market their services or circulate a survey. You must not release this information but instead can offer to mail the information/survey on their behalf. If you do decide to undertake a host mailing, you should include a statement explaining the context of the mailing and reassuring Tenants that their personal data have not been released to the third party. Tenants are given an opportunity to opt out of such mailings when they become a Tenant of the Association and Association systems are designed to take this into account.

Section 9: Forwarding Tenant Correspondence on behalf of a Third Party

You should not release Tenant addresses or contact details to a third party without the consent of the Tenant. Instead you may offer to forward correspondence to a Tenant on behalf of a third party. Sometimes you may even receive unsolicited

correspondence with a request to forward it to a Tenant. You must take care when handling such requests. Remember that an individual's Tenant status is personal data. Therefore if you receive such a request it is important to neither confirm nor deny that that person is a Tenant at the Association.

V Telephone Protocol for the Disclosure of Personal Data

The Association must ensure that personal data held on individuals are not disclosed to unauthorised third parties including family members, friends, government bodies and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data to third parties. These guidance notes are intended to provide guidance for staff who deal regularly with telephone calls from third parties requesting personal data on Tenants and staff and should be read in conjunction with the Association's Data Protection Policy. This document is Appendix VI to the policy.

Section
1. General Information on Disclosure of Personal Data.
Disclosing Personal Data / Disclosing Sensitive Personal Data / Disclosing Personal Data Overseas /Consent.
2. Internal (within Association) Disclosures by Telephone.
3. External (outside Association) Disclosures by Telephone.
General / Disclosure to Parents (Tenant Information) / What to do if someone calls claiming to be a Tenant / Home Addresses, Telephone Numbers and E-mail addresses / References / Disclosures to the Police
4. Conclusion

Section 1: General Information on Disclosure of Personal Data

Disclosing Personal Data

In accordance with Principle 1 of the Data Protection Act, personal data should only be disclosed if one of the conditions set out in Schedule 2 are met. The most likely conditions applicable to the disclosure (over the telephone) of Tenant or staff data to third parties are:

- the Tenant or member of staff has given their consent.
- the disclosure is in the legitimate interests of the Association or the third party to whom the information is being disclosed (except where this would prejudice the rights, freedoms or legitimate rights of the Tenant or member of staff).
- disclosure is required for performance of a contract

Disclosing Sensitive Personal Data

In accordance with Principle 1 of the Data Protection Act, sensitive personal data (racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions) should only be disclosed if one of the conditions set out in Schedule 2 (see above) AND one of the conditions set out in Schedule 3 are met. The most likely conditions (of Schedule 3) applicable to the disclosure (over the telephone) of sensitive Tenant or staff data to third parties are:

- the Tenant or member of staff has given their explicit written consent.

- disclosure is in the vital interests of the Tenant or member of staff (eg information relating to a medical condition may be disclosed in a life or death situation).

Disclosing Personal Data Overseas

In accordance with Principle 8 of the Data Protection Act, personal data should only be disclosed outside of the EEA (the EU Member States together with Iceland, Liechtenstein and Norway) if one of the conditions set out in Schedule 4 are met. The most likely conditions applicable to the disclosure (over the telephone) of Tenant or staff data to third parties overseas are:

- the Tenant or member of staff has given their explicit (ideally written) consent.
- disclosure is required for performance of a contract.
- disclosure is necessary for the purpose of any legal proceedings.

Consent

The Association understands "consent" to mean that the Tenant or member of staff has signified their agreement whilst being in a fit state of mind to do so and without pressure being exerted upon them. There must be some active communication between the parties, consent cannot be inferred from non-response to a communication. In most cases, verbal consent should be acceptable so long as proper security checks are made to ensure that the person giving the consent is the Tenant or member of staff. For telephone consent, this will mean asking the subject to confirm several separate facts that should be privy only to them (Tenant identity number, telephone number, date of birth etc). For sensitive data, consent should NOT be obtained over the telephone and explicit written consent of Tenants or staff should be obtained unless an alternative legitimate basis for processing exists (see above).

Section 2: Internal (within Association) Disclosures by Telephone

You should always think carefully before disclosing Tenant or staff personal information to work colleagues whether they be from within, or external to, your own department. Under the Data Protection Act, you should not disclose personal data to colleagues unless they have a legitimate interest in the data concerned. As there is no definition as to what a "legitimate interest" is, it will have to be a matter of judgement in each case. As a rule you should consider whether or not the information is necessary to allow your colleague to perform their job. When sharing information with colleagues, you should consider the level of detail necessary to enable them to perform their job.

If you can identify the member of staff making the telephone enquiry (eg from their voice) and you are satisfied that they have a legitimate reason for requesting the personal information, you may disclose this over the telephone. Take care to ensure that in disclosing the information over the phone, you are not inadvertently disclosing the information to other members of staff. This is particularly important in the case of sensitive personal data and for staff working in an open plan office.

If you cannot be sure of the identity of the member of staff making the telephone enquiry, you should ask them to put the request in writing (email is preferable) so that you can deal with it at a later stage. Again, before releasing the information, you need to be satisfied that the member of staff is requesting the data for a legitimate purpose. Ask the enquirer to indicate what they will be using the information for and keep the written communication as background evidence should the disclosure be questioned at a later date. To avoid embarrassment you could say that you do not have the information to hand and that you need time to find it and get back to them. Alternatively you could offer to take a contact telephone number and call them back later once you have gathered the information.

Section 3: External (outside Association) Disclosures by Telephone

General

In general, disclosures to external bodies/companies/agencies/individuals should not be made over the telephone. It is strongly advised that you ask enquirers to submit their requests in writing (where appropriate on headed paper). This will give you time to check whether or not the request is legitimate and where possible obtain consent for the disclosure from the member of staff or Tenant about whom information is requested. You should, wherever possible, reply to the request in writing.

The Association recognises that in some, exceptional situations, time constraints and other factors make it a necessity to disclose information over the telephone. Good practice is considered to be only releasing information to those individuals who have access to a unique identifier (Tenant number) or know at least 3 identifying data (e.g. name, address and date of birth) about the data subject. This should minimise the potential for damages because a relationship between the data subject and the caller has been established. If you find yourself in a position where it is necessary to disclose information over the telephone, you should take a contact number and ring the enquirer back. This will go some way to ensuring that the caller is who they say they are. Even the above procedures could be subject to fraud and should only be used when no other alternative exists. In such cases, the Association should at least be regarded as having taken reasonable precaution given the circumstances - i.e. that the security in place was appropriate to the risk involved in unlawful processing of data. As always, particular care should be taken when disclosing sensitive personal data or information that could potentially cause the Tenant or member of staff to suffer subsequent damage and/or distress.

Please note that even confirming whether or not a Tenant or member of staff is a tenant of or works at the Association could be a potential breach of the Act.

Disclosure to Parents (Tenant Information)

The Association has no responsibility or obligation to disclose any personal information relating to Tenants to parents or other relatives, even if they are contributing to rent.

All Tenants are given the opportunity to provide the name of a nominated individual to whom the Association may disclose personal information. You should always check a Tenant's record to see whether or not they have identified a nominated individual. You may come under pressure to discuss individual Tenants with parents/guardians or even friends over the telephone. However, in these situations it is essential that you do not disclose personal data without the prior consent of the Tenant - it would be a breach of the Data Protection Act to do so. If the Tenant has identified a nominated individual (see above) they are understood to have given prior consent.

You are, of course, free to discuss Association procedures with parents but the specific circumstances of an individual Tenant cannot be discussed without the consent of that Tenant.

There may be occasional, exceptional circumstances (in which a Tenant's life or health is threatened) in which the usual need to get consent before disclosing to parents/guardians may be waived. The Association holds details of Tenants' "next of kin" for such purposes.

What to do if someone calls claiming to be a Tenant

You may receive telephone calls from individuals claiming to be Tenants and asking, for example, for their rent balance. Unless you are 100% sure that the person on the line is who they claim to be, you should not disclose information over the telephone. You are advised to ask for confirmation of the Tenant's id number, home address and date of birth before proceeding with the call. If the caller can provide the details accurately, make a note of the information that they require and inform them that you will send it to their address recorded on the Association database. If the caller insists that they need the information urgently, you may take a contact telephone number and call them back with the information.

Home Addresses, Telephone Numbers and E-mail addresses

You should never give out personal/home addresses or telephone numbers of staff or Tenants to third parties over the telephone unless you have been given explicit (in writing) permission by the individual. Instead you could a) take the caller's contact details and say you will pass a message asking the Tenant or member of staff to contact them if they are in the Association or b) offer to forward correspondence to a Tenant or a member of staff on behalf of the caller. You must take care when handling such requests. Remember that an individual's Tenant/staff status is personal data. Therefore if you receive such a request it is important to neither confirm nor deny that that person is a Tenant or member of staff at the Association.

However, it would usually be deemed appropriate to disclose a colleague's work contact (telephone and departmental address) details in response to an enquiry regarding a particular function for which they are responsible. If you are asked to disclose another member of staff's email address, you should ask the caller to send the email to you and inform them that you will forward the message on to the individual they are trying to contact if they are a member of the Association. It would

not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter.

References

Telephone references are not usually recommended. However, they are acceptable if you have been specifically asked by a Tenant or a member of staff to provide a reference at short notice. The identity of the person requesting the reference should always be confirmed prior to disclosure. As a minimum security measure it is recommended that you ring the enquirer back to check that they are who they claim to be.

When disclosing information in the form of a personal reference ensure that:

1. the information you disclose is FACTUALLY correct;
2. the disclosure is kept to a minimum;
3. sensitive data (e.g. details of health to explain absences from work) are not disclosed without the explicit consent of the member of staff;
4. where opinions about a person's suitability are disclosed, your comments are defensible and justifiable on reasonable grounds;
5. if you are unable or unwilling to give a reference, such a refusal is communicated carefully, without, in effect, implying a negative reference.

Disclosures to the Police

Disclosures to the Police are NOT compulsory except in cases where the Association is served with a Court Order requiring information. However, Section 29 of the Data Protection Act 1998 does allow the Association to release information to the Police WITHOUT the consent of Tenants or members of staff in LIMITED circumstances. Such disclosures should only be made if the Police confirm that they wish to contact a named individual about a specific criminal investigation and where the Association believes that failure to release the information would prejudice the investigation. If you are contacted by the Police and are not sure how to deal with their request you can get in touch with the Chief Executive for advice on how to deal with the enquiry.

The Police MUST request the information from the Association in writing. You are NOT obliged to release information to the Police over the telephone. Most Police Forces will have their own request form, which should always include:

1. a statement confirming that the information requested is required for the purposes covered in Section 29;
2. a brief outline of the nature of the investigation;
3. the data subject's role in that investigation;
4. the signature of the investigating officer.

Section 4: Conclusion

The purpose of the Data Protection Act 1998 is to protect the rights and privacy of individuals with regard to their personal information. At times you may feel like you are being obstructive to callers asking for information about Tenants or members of staff. In these cases, explain that the information falls under the Data Protection Act.

Follow the above guidelines in a courteous and professional manner and in most circumstances you should not experience too many problems. However, if you are faced with a particularly difficult caller, do your best to diffuse the situation without losing your temper. Explain that you are following guidelines approved by the Association and that by providing the information over the telephone, you could be breaking the law.

Remember:

There is no such thing as a Data Protection emergency (except where someone's life or health may be at risk). You are well within your rights to stall a caller whilst you seek further information and advice.

VI References

These guidance notes cover the provision and receipt of references for both staff and Tenants and should be read in conjunction with the Association's Data Protection Policy.

Section 1: General

Many staff in the Association may, in the course of their career, be asked to provide references for Tenants and/or members of staff, whose future housing provision/careers they are in a position to influence. This will involve the disclosure of personal data in the form of facts and opinions about individuals and as such is covered by the Data Protection Act 1998.

There are a number of types of references including:

- standard references for employment or placement at another Housing Association
- references for internal candidates regarding their employment/promotion
- character references for legal proceedings
- financial references for mortgage applications

All types of references fall under the definition of personal data and sometimes sensitive personal information (e.g. relating to health, race, religion - see Data Protection Policy section on definitions for full details of what data the Act considers to be sensitive), in the Data Protection Act. Therefore staff should ensure that they are fully aware of the implications of the Act when providing references, this includes appropriately secure storage of references both received by and provided by the Association.

Section 2: Guidance on Writing a Reference

Particular care should be taken if asked to provide a reference for someone who is not known to you.

If you receive a request for a personal reference relating to a member of staff or a Tenant, you should ensure that:

1. the information contained in the reference is FACTUALLY correct
2. where possible, disclosure is kept to a minimum

3. sensitive data (e.g. details of health) must not be disclosed without the explicit consent of the member of staff or tenant (if this is not possible, please contact the Association's Chief Executive for advice)
4. where opinions about a person's suitability are disclosed, your comments are defensible and justifiable on reasonable grounds
5. if you are asked to express an opinion on an issue about which you have limited knowledge, e.g. honesty and integrity, you respond appropriately response (for example, "I know of nothing that would lead me to question X's honesty")
6. if you are unable or unwilling to give a reference, such a refusal is communicated carefully, without, in effect, implying a negative reference
7. you do not disclose any information if asked to give an unsolicited reference (i.e. for a Tenant or member of staff who has not, to your knowledge, cited your name as a referee) without the individual's consent.

Section 3: Permission to Disclose Information in the form of a Reference

If a member of staff or Tenant has provided the name of a referee, the Association interprets them as having given their consent for the disclosure of personal information in the form of a reference. However, if you are intending to release sensitive personal information (e.g. relating to health, race, religion - see Data Protection Policy section on definitions for full details of what data the Act considers to be sensitive), you should always seek explicit consent (preferably in writing) from the individual concerned. As a matter of good practice and courtesy, members of staff and Tenants should be encouraged to inform people that they intend to cite them as a referee.

In some cases, requests for references may be presented on a pro-forma already signed by the individual permitting you to disclose information in the form of a personal reference. You should be able to satisfy yourself that the signature on the form is genuinely that of the individual concerned before proceeding with the request.

The identity of the person requesting the reference should always be confirmed prior to disclosure. Requests for references should usually be made in writing on headed paper. If you receive an email request for a reference, you should be assured that it is a valid request. If it is from a known source or company, you should process the request but you may wish to reply in written format to a known postal address for the company/organisation. If the email address is not familiar, you are advised to investigate further.

Telephone references are not recommended.

Section 4: Rights of Access to Confidential References

4.1 References RECEIVED BY the Association

All staff should be aware that the Data Protection Act gives individuals the right to access information that an organisation holds on them. Such requests are known as subject access requests. This includes references received by the Association which are stored in staff or Tenant files. However, when releasing references to individuals upon receipt of a subject access request, staff need to be mindful that they are not inadvertently disclosing information relating to a third party (e.g. the referee) without their consent. For further information on obtaining consent for the release of third party data in response to a subject access request, see guidance on Handling Subject Access Requests.

With this in mind, you should be aware of the following issues regarding retention of references received:

- References for successful staff appointments must be retained for 12 months after appointment. You may need to communicate this to referees when requesting references.
- References for unsuccessful candidates should be retained for a period of up to 12 months (in case of possible litigation from unsuccessful applicants). You may need to communicate this to referees when requesting references.

Some organisations invite the referee to state if s(he) has any objection to the reference being disclosed to the candidate. However, only in very rare cases will this be possible and usually the candidate will have a right to see their reference albeit it with referees' personal details removed. See Section 5 for further detail.

4.2 References PROVIDED BY the Association

References are exempt from subject access requests in the hands of the originating data controller (i.e. the Association). However, the Act does not stop the disclosure of such references and all departments are encouraged to be as open and transparent as possible regarding the information they hold on individuals (staff and tenants). Also remember that individuals could request the reference from the RECEIVING organisation. As a general rule, you are advised not to include information in a reference that you would not wish to the individual concerned to see. Where opinions about a person's suitability are disclosed, make sure your comments are defensible and justifiable on reasonable grounds so that you do not cause unnecessary distress in the event of your reference being viewed by the individual.

4.3 Internal References

Arguably, internal references are both provided by and received by the same organisation which gives rise to some uncertainty about the extent to which the exemption described in 4.2 applies. Again, it is stressed that staff should aim to be as open and transparent about the information held on individuals. When providing internal references, staff are reminded that individuals may be able to access them. Where disputes arise as to whether or not an individual should be allowed access to references provided to the Association from the Association, cases will be dealt with on an individual basis taking full account of the specific details in each case. You should consult the Association's Chief Executive if you have any concerns.

Section 5: Requesting References

When requesting a reference (as an employer / provider of education) from external or internal referees you may wish to:

1. inform them of the Association's policy on retaining references (12 months for both successful and unsuccessful candidates)
2. inform them that in the event of a subject access request, wherever possible their personal data will not be disclosed without consent but where the Association considers it to be reasonable, it may be necessary to release references without consent
3. that references will be accessible if requested in connection with legal proceedings or in connection with the detection or prevention of crime.
4.

Please be aware that this might affect the nature of references received by the Association. All staff are reminded that telephone references are not recommended Association practice.

VII Guidance for Photographs to be used in Publicity/Promotional Material

These guidance notes cover the provision and receipt of references for both staff and tenants and should be read in conjunction with the Association's Data Protection Policy.

General Photographs

If individuals are not readily identifiable from the photograph and it seems unlikely that any damage or distress will result from such processing then it will not be necessary to obtain consent. Therefore, tenants and staff whose images appear as incidental detail in publicity photographs will not need to give consent for the use of their image.

Photographs of Group Activities

Where photographs are to be taken of a group activity (e.g. a seminar) then this should be announced in advance so that individuals may leave the room briefly if they do not wish to appear in the photographs.

Photographs of Small Groups/Individuals

Where photographs are to be taken of a single individual, or a small group of individuals, where individuals are the main subject of the photograph (even if they are not identified by name), consent should be sought before any photographs are taken. When gaining consent, it is important to ensure that individuals are informed of what the images will be used for (e.g. where they will be printed and who will have access to them). In most cases, verbal consent is all that will be required.

Publishing Photographs on the Web

If it is intended to make photographs available on the web, wherever possible this should be restricted to the Intranet rather than the Internet. Publishing on the Internet potentially transfers personal data outside of the EEA (the EU Member States together with Iceland, Liechtenstein and Norway) for which rules on gaining consent from individuals are much stricter. If photographs (except where tenant/staff images appear as incidental detail) are to be published on the Internet, written consent should be obtained from the subject(s). The Association will make reasonable efforts to ensure that such consent has been obtained before use and where this is not possible will avoid use where it may reasonably be considered likely to cause the data subject damage or distress. The Association will also respond promptly to any subsequent request to remove a photograph from the web site by an individual who is clearly identifiable in that image.