HousingExecutive

Procedures for Handling Personal Information under the Data Protection Act 1998

1.0 SCOPE OF THE PROCEDURES

These procedures for the collection and handling of personal information apply to all personal information created or collected by the Housing Executive and its staff in the course of their daily work.

The information includes:

- The names and other details of tenants, grant applicants, housing benefit claimants, employees, and other individuals with whom we do business;
- The names and other details of those who correspond with us or provide details during telephone calls;
- Information about contractors and suppliers of goods and services;
- Information held by managers about their staff, such as performance management information;
- Word processed documents, spreadsheets and databases which contain personal details such as names and addresses
- Emails, where either the person sending or receiving is identifiable or the contents refer to identifiable people

Collectively this personal information is called 'personal data' and the people it is about are called 'data subjects'. The information is generally held in computer systems such as HMS, I-world (HB), Payroll and PSMS (Grants), Outlook mailboxes, and a range of other local specific databases 'owned' by other Departments.

The general rule to be followed is to handle and use information about other people as carefully as you would wish information about yourself to be handled and used. These procedures are an expansion of that general rule.

2.0 GLOSSARY

2.1 Redaction

The removal of data that is exempt by whatever means is required, for example, using black marker pen on both sides of the paper, or blanking out after photocopying the document. The original document must not be altered in any way.

2.2 Data

Information about individuals which is:

- Processed on computer and in manual form
- Recorded with the intention of processing on computer or manually
- Recorded and kept electronically or manually.
- Or is recorded information held by a public authority and does not fall within

2.3 Data Subject

Any individual who is the subject of personal data. This includes:

- Customers, their partners and dependants
- NIHE Staff

All references to the data subject should be understood to mean the data subject or their legal representative.

2.4 European Economic Area

The European Economic Area (EEA) consists of the European Union (EU) Member States together with Iceland, Liechtenstein and Norway. Under EEA Gibraltar is part of Great Britain. The Isle of Man and the Channel Islands are not part of the EEA.

2.5 Effective date (In relation to a Subject Access Request)

The date on which a Subject Access Request (SAR) is received in any Housing Executive office with sufficient information to identify the data subject and the location of the data requested.

2.6 Enforcement Notice

Notice served by the Information Commissioner to compel a data controller to take a specific course of action in relation to the processing of data.

2.7 Exempt data

Certain data, which can be legally withheld when responding to a Subject Access Request (SAR), and which relates to:

- crime and taxation
- medical information
- research, history and statistics

Full details of categories of exemptions can be found in the Act (see section 27 to 39 of the Act).

2.8 External transfer

The passing of the SAR to another public body. On transfer to another public body the Housing Executive is no longer responsible for responding to the SAR.

2.9 Information Commissioner

Independent officer, appointed by Her Majesty the Queen, who reports directly to Parliament. The Commissioner was previously named the Data Protection Registrar under the Data Protection Act 1984.

2.10 Personal data

Data relating to a living individual who can be identified, either by the data alone or with other information or opinion held by the data controller or information likely to come into the possession of the data controller.

2.11 Potential SAR

This term relates to a SAR which does not have sufficient information to enable the Records Manager to confirm the identity of the data subject.

2.12 Processing (In relation to data)

Throughout the Data Protection Manual, "processing data" is defined as obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including:

- Organisation, adaptation or alteration of the data
- Retrieval, consultation or use of the information
- Disclosure of the data by transmission, dissemination or otherwise making available
- Alignment, combination, blocking, erasure or destruction of the data

2.13 Sensitive Personal Data

Personal data consisting of information as to:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Their physical or mental health or condition
- Their sexual life
- The commission or alleged commission by them of any offence
- Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

2.14 Special Purposes

The processing is undertaken with a view to publication by any person of any journalistic, literary or artistic material (see section 32 of the Act).

2.15 Subject Access Request (SAR)

Formal written or e-mail request received from the data subject for sight of or a copy of their data record(s) held by the Housing Executive.

2.16 Subject Access Fee

Payment of the standard Subject Access Fee of £10 must be received before the Housing Executive will process a Subject Access Request

3.0 DATA PROTECTION POLICY STATEMENT

3.1 Introduction

This policy statement sets out how the Housing Executive implements the Data Protection Act 1998 (The Act). The Act was brought into force on 1st March 2000, replacing the 1984 Act. Its scope was extended by the Freedom of Information Act 2000.

The Housing Executive collects and uses information about the people with whom we deal. We also acquire information about others in the course of those dealings. These people – collectively called 'data subjects' – include our own staff, applicants for housing and renovation grants etc. The information can be factual information, such as name and address, or expressions of opinion about or intentions towards individuals. It can occur in any format – Word documents, databases and spreadsheets, emails, CCTV, index cards, paper files.

This policy statement applies to all personal data acquired, held and used by all constituent parts of the Housing Executive.

3.2 Background

The Data Protection Act 1998 (DPA) came into force on 1st March 2000. It supersedes and extends the provisions of the Data Protection Act 1984. The new Act implements a European Directive of 1995 and has two aims:

- to protect individuals' fundamental rights and freedoms, notably privacy rights, in respect of personal data processing
- to enable organisations to process personal information in the course of their legitimate business

The Act applies to any processing of personal information. Processing includes virtually anything that can be done to information, including acquisition, storage and destruction as well as active use.

Personal data held by the Housing Executive is subject to the Data Protection Act if it is recorded information and it relates to an identifiable living individual.

Individuals have the right, upon written request, to be informed whether or not information about them is being processed by us; to be given a description of the information, the purpose of our processing and to whom it may be disclosed; and to be provided with the information in intelligible form. We have the right to charge a fee for this and the fee is set at £10 in the Data Protection Regulations.

We are obliged to follow certain procedures and to comply with the eight Data Protection Principles unless the personal data is exempt. These Principles (which are set out in Schedule 1 to the Act) require that personal information be handled as follows:

Principle.1

It shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

Principle.2

It shall be obtained only for one or more specified and lawful purpose, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Principle.3

It shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed

Principle.4

It shall be accurate and, where relevant, kept up to date

Principle.5

It shall not be kept for longer than is necessary for that purpose or those purposes

Principle.6

It shall be processed in accordance with the rights of data subjects under the Act

Principle.7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

Principle.8

It shall not be transferred to a country or 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

There are sanctions to ensure compliance: the Information Commissioner has powers to enter premises where an offence under the Act is suspected of having been committed and to inspect or seize material. The Commissioner also has the right to prosecute offenders and compensation may be payable.

3.3 The Housing Executive's Commitment to Data Protection

The Housing Executive is committed to full compliance with the Data Protection Act 1998. We regard responsible handling of personal information as a fundamental obligation and one that is in keeping with our role as the comprehensive housing authority for Northern Ireland. To this end we endorse and adhere to the data Protection Principles as set out above.

Housing Executive staff are expected to do whatever is necessary to ensure compliance with the Data Protection Act 1998, and in particular to adhere to our Data Protection Procedures as set out in this manual.

4.0 MANAGING PERSONAL DATA AS RECORDS

4.1 Introduction

Personal data created, obtained and held by Housing Executive staff as a result of their work are part of our corporate records. They are subject to the procedures and business rules governing the management of records outlined in our Records Management Handbook and Meridio Policy and Procedures guidelines.

As a general rule, the Housing Executive's Records Manager should be consulted about the retention and destruction of sets of personal data. However, it is the responsibility of each member of staff to ensure that:

- Incoming and outgoing emails are either filed or deleted once the action to which they relate has taken place, if not earlier. Those which remain in a personal mailbox pending a final decision should be reviewed at regular intervals and either filed or deleted. All emails will be deleted from personal mailboxes by system action after 12months
- The contents of personal folders should be reviewed at regular intervals. Any documents which should form part of our corporate record should be filed in Meridio; and anything no longer needed should be deleted.

5.0 OBTAINING PERSONAL DATA

This section sets out good practice to be followed when acquiring personal information.

5.1 Be selective

Consider what personal information you need to collect to achieve your objective, keep a record of your decision and ensure that you collect only that information. Do not collect irrelevant information simply because it might be useful at some point in the future. Consider whether depersonalised or anonymous information would achieve the same result as information with a name attached.

5.2 Be open and honest

Be as transparent and candid as possible when acquiring personal information from people. One method of ensuring this is to ensure that any form or screen used to obtain personal data includes the following:

- The identity of the data controller. Our name, in full as 'The Housing Executive', should appear somewhere.
- A brief description of the purposes for which the information will be used. This can be a phrase or sentence such as 'This information will be used only to process your job application'. If you intend to make any additional use of the information see section 3.3.
- A brief description of any proposed disclosure of the information to third parties and, if so, an opportunity for the person to give or refuse consent to this (see section 3.3 for details)

- A statement that people have the right of access to information about them and the right to seek its correction

This is a 'fair processing notice' and must be reasonably intelligible, in reasonably prominent type, and in a reasonably prominent position on the relevant form or screen. It could be along the following lines:

The information that you provide will be processed in accordance with the provisions of the Data Protection Act -1998 and relevant legislation. The Housing Executive has a duty to protect public funds it administers, and may use information held about you for the prevention and detection of fraud and other lawful purposes. The Housing Executive will also use the information for the purpose of performing any of its statutory duties. It will make any disclosures required by law and may also share this information with other bodies responsible for detecting / preventing fraud or auditing / administering public funds. We will not disclose your personal information to third parties for marketing purposes.

If information required for one purpose is being obtained during a telephone call, and there is any intention to use it for any further purpose, the person must be informed and asked to consent to this. Any granting or refusal of consent should be recorded and held on a relevant file.

If the data being collected is 'sensitive' personal data, you must either obtain the consent of the data subject, or establish grounds for carrying out the processing under Schedule 3 of the Act. With sensitive personal data, consent must be active and you cannot infer consent from a failure to respond. You cannot assume consent just because people have not clearly refused it. Retain the evidence of consent for as long as you keep the personal information

5.3 Be careful in creating personal data

Do not make adverse comments about individuals unless they are based on recorded facts and can be defended as accurate if challenged. Whenever you write anything about individuals, remember that they have a right to ask to see what is written about them.

5.4 New sets of data

If you are collecting a new set of data, it may be necessary to record this in the Information Asset Register. For further advice contact the IT Security Manager, IT Department, or the Records Manager, Corporate Services. This requirement does not apply to personal mailboxes and contact lists maintained by individuals for occasional personal use.

6.0 HOLDING AND USING PERSONAL DATA

This section sets out good practice to be followed when processing personal information. Processing includes holding and storing as well as actively using.

6.1 Be able to justify processing of personal data

Processing must always be

- Personal data must be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
- If you do not have consent but you can link your processing to any of the Housing Executive's statutory functions, objectives or targets in our current corporate and business plan, then you can reasonably assume that your processing is justified on the grounds that it is necessary for us to carry out our functions. If you do not have consent or cannot make this link but need to process personal data, consult the Data Protection Officer before you start processing.

6.2 Compatible processing

Personal information should be used only for the purpose(s) for which it was obtained or for compatible purposes. For example, information collected for research purposes cannot automatically be used for other non-related purposes unless the data subject has consented to this different use.

6.3 Processing sensitive data

You need to be particularly careful if you are processing sensitive personal data. As well as being fair to the person the information is about, and lawful, you must be able to justify use of the personal information against one of the justifications described above, i.e. we have consent of the data subject or processing is essential for carrying out our functions, or one of the following justifications applies:

- Processing is lawfully required for employment purposes
- The information has already been made public by the person concerned
- Processing is needed for legal proceedings, to obtain legal advice or to establish or defend legal rights
- Processing is needed for ethnic monitoring
- Processing is necessary to protect the vital interests of the data subject or another person and obtaining consent is not an option
- Processing is necessary for research purposes, will not involve making decisions about the data subjects and is unlikely to cause them substantial damage or distress

If none of these justifications can be used but you do need to process sensitive personal data, consult the Data Protection Officer before you start processing.

7.0 KEEPING PERSONAL DATA ACCURATE

This section explains the importance of keeping personal information accurate and up to date and what you should do about correcting inaccurate information.

7.1 Personal information should be accurate and up-to-date

Any personal information that you are processing should be accurate and up-to-date. The difficulties of ensuring total accuracy are recognised and a realistic approach is adopted in the Act by requiring 'reasonable' steps to have been taken to ensure accuracy. A relevant factor is whether the person will be disadvantaged by your processing. The more this is likely, the more careful you should be about accuracy.

Keep a record of the procedures you adopt for checking the accuracy of the data you obtain and process.

7.2 Requests for correction of personal data

People have the right to seek correction of personal information about them. If someone states that information about them is inaccurate and can provide evidence to support this, the correction should be made.

Depending on the nature of the information, it may be necessary to record the fact of the correction and retain the incorrect data. For example, a simple change of address may require no formal record of amendment but something more complex that could affect the rights of the person concerned should be recorded and the incorrect information previously used for decision-making should be retained. If you think there is any likelihood that you might need to refer to the previous version, or be asked when it was corrected, keep a record of the correction, for example by adding a note 'corrected on <the date>' and signing it, if it is a paper record, or by filing a note in Meridio.

If the change requested is complicated, or relates to information that is in any way disadvantageous to the data subject or to information that is not in current use, consult the Data Protection Officer.

We do not normally correct data held in archive storage. If such a request is received, refer it to the Data Protection Officer.

7.3 Inform third parties of corrections to personal information

If you are correcting personal information consider whether it might have been passed to another Housing Executive department and, if so, whether they should be informed of the correction.

If the information was disclosed to a third party some years ago for a specific purpose, for example in connection with a job application, then sending a correction is unlikely to be necessary. If in doubt, consult the Data Protection Officer.

8.0 RETAINING OR DESTROYING PERSONAL DATA

This section sets out the need to make decisions about keeping or destroying personal information and to implement those decisions.

8.1 Make retention/destruction decisions

As a general rule, do not keep personal information for longer than necessary. Unless you are retaining it as part of the corporate record, or you have a specific reason for keeping it, destroy or delete it when you no longer need it for the purpose for which it was obtained. This includes emails in personal or shared mailboxes, which should either be filed in Meridio or deleted. It is particularly important that emails containing sensitive personal data, for example information about someone's health, are not kept in mailboxes indefinitely. (Note that emails that remain in mailboxes are deleted automatically after twelve months.)

If personal information is being kept for the corporate record, make sure it is included in disposal schedules agreed with the Records Manager and that it is destroyed in accordance with normal application of such schedules.

9.0 KEEPING PERSONAL DATA SECURE

This section gives some basic guidelines about the safekeeping of personal information. See also the Housing Executive's Information Security Handbook for more detailed guidance.

Guide to Document & IT Security

9.1 Store personal information securely

It is very important that personal information is stored securely and access restricted to those with a need or right to see it. This is particularly the case if sensitive personal data is involved, or sets of information about a number of people.

Make sure that personal information held by you is not disclosed either orally or in writing, whether accidentally or not, to any unauthorised third party by taking the following measures:

- Do not leave paper copies of personal information where anyone else can access them. Keep manual personal records locked away securely
- If you hold personal information on your computer, do not leave it unattended without locking the computer; do this also if you have a visitor who should not see the information on your screen
- If the personal information is filed in Meridio, set access controls so that it can be accessed only by those with a need and a right to see it.
- If the personal information is held outside Meridio and is not common knowledge, use passwords to secure it

9.2 Transmit personal information securely

Ensure that transmission of information, whether internally or externally, is done with a level of security appropriate to the nature of the information.

If the information is being transmitted within The Housing Executive by physical means, such as in an envelope, ensure the envelope is sealed and alert the recipient to the fact that you have despatched it. Ask the intended recipient to provide email/telephone

confirmation of receipt. If it is being transmitted by email, ensure the email is marked with appropriate Protective marking.

If sensitive personal data is being transmitted externally by electronic means; e.g. to a contractor or other public body, the following rules apply:

- Ensure the transmission has been approved by the Information Asset owner (usually an Assistant Director)
- Use technical means such as encryption for transmission
- If a password is required, send it separately

See also the Housing Executive's 'Out of Office Security Policy' for further guidance on the handling of personal data and other sensitive information when outside the office;

Out of Office Security Policy

9.3 Retrieval of files from archive storage

The 7th Data Protection Principal required the Housing Executive to take appropriate technical and organisational measures in order to avoid the loss of, or unauthorised access to, personal data.

Files held in archive storage containing personal data, or other business sensitive information, should be managed in a way that restricts access only to those individuals who are properly authorised to do so.

When requesting retrieval of files containing this type of sensitive information, care should be taken to ensure that, once the files are delivered from the store, they are delivered promptly to the individual officer who made the request. If it is not possible to deliver them immediately (for example the requesting officer is out of the office), the files should be held in a secure area (e.g. locked cabinet, office or store room? Until such time as they can be delivered to the appropriate officer.

Bear in mind that the person delivering the files will not necessarily be aware of the sensitive nature of their contents. The onus is, therefore, on the owner of the files (in this case the requestor) to ensure that appropriate arrangements are I place for the secure handling of the files from the point when they are delivered until they are returned to archive storage.

9.4 Phone calls

Phone calls can lead to unauthorised use or disclosure of personal information and the following precautions should be taken:

- If you receive a phone call asking for personal information to be checked or confirmed, be aware that the phone call may come from someone pretending to be the data subject, or impersonating someone with a right of access, and check their identity
- If a phone call requires authorised disclosure of personal information but in circumstances that would lead to people sitting close to you overhearing it, move the phone conversation to a room where you can have privacy

Please note that the above rules only apply to enquiries relating to personal data of a routine nature e.g. a tenant making enquiries about rent payments etc. All other requests for disclosure of personal data should be treated as Subject Access Requests and should be made in writing. If in doubt, seek advice from the Data Protection Officer

9.5 Avoid loss, unplanned destruction or damage

Ensure that unauthorised or accidental access, alteration, disclosure, destruction or loss of significant sets of personal information is kept to a minimum and, if it happens, that you record the circumstances and report the incident to the Security Officer, I.T. Department, Headquarters.

9.6 Destroy information securely

When deleting information held electronically, ensure that it is removed from the Recycle Bin. Destroy paper-based personal information only under secure conditions - shred it or use a Confidential Waste bag. Further advice on this is available from the relevant Facilities Services Manager.

10.0 SHARING PERSONAL DATA WITH OTHERS

This section explains precautions to take if passing personal data to another person or organisation.

Do not pass personal data to anyone outside The Housing Executive without having first obtained approval from either an Assistant Director, Area manager or Level 9, unless it is through existing approved data sharing arrangements.

If personal data is being passed to someone outside The Housing Executive, follow the guidance at below, and keep a record including:

- Sufficient details of the information for it to be clearly identifiable subsequently
- The name of the person who has authorised it
- Details of to whom is has been sent
- The date on which it was sent
- The means used to send it, e.g. encrypted email

The guidance above is suitable for situations where the information sharing relates to a single individual or small numbers of individuals in a one-off situation. If you are considering sharing information on a larger scale, or smaller amounts of data but on a regular basis then you should consider managing this process via a Data Sharing Agreement; and the following section gives guidance in this area.

10.1 The Information Commissioner's View on Data Sharing

Information sharing should be supported by a sound business case, preferably accompanied by a Privacy Impact Assessment. This should identify the intended benefits and demonstrate that the data protection risks have been identified and addressed.

ICO view on Information Sharing - link in ICO down.

Data Sharing Agreements

Business units considering entering into new data sharing arrangements, and those currently sharing data, are encouraged to formalise such information sharing in a formal 'Data Sharing Agreement'.

Detailed guidance on this topic has been supplied by the information Commissioner in his document 'Framework Code of Practice for Sharing Personal Information', which can be viewed her

ICO Data Sharing Code of Practice

ICO Data Sharing Checklist

It is a requirement that all data sharing should be registered in the Housing Executive's Data Transfer Register which is maintained by the IT Security Officer, IT Department, Headquarters.

11.0 DATA SUBJECT ACCESS AND OTHER RIGHTS

This section outlines the rights of data subjects and how to respond to them.

11.1 Data subjects have certain access rights:

- To be told whether information about them is being processed
- To be given a description of the information and the purpose for which it is being processed and details of others to whom it is or has been disclosed
- To see the information in intelligible form
- To be told how it was obtained

To be valid, requests must be in writing, either on a form such as the NIHE Data Protection leaflet or in a letter or email. Anyone making an oral request should be asked to put it in writing and a copy of the form should be offered.

Personal information should not be given out to a data subject over the telephone unless you have no doubts as their identity and the information is innocuous. For telephone enquiries, check the requested information. If it seems innocuous and the enquirer is able to answer a question from it, take the callers number, call them back and provide the information; but if you have any doubts, ask the caller to put their enquiry in writing.

Requests may also be received from NIHE staff for access to personnel records.

The Housing Executive will require payment of the subject access fee in all cases (including NIHE staff) before it will process a subject access request. The Data Protection Regulations permit a data controller to charge a maximum fee of £10 for processing a Subject Assess Request.

12.0 SUBJECT ACCESS REQUEST MANAGEMENT PROCEDURES

12.1 What is a Subject Access Request?

The Data Protection Act 1998 (The Act) gives data subjects the right of access to data. This applies to the following:

- Customers and their representatives
- Staff as employees or customers.

A request for personal data is a Subject Access Request (SAR) and it must be managed in compliance with the requirements of Section 7of the Act (Right of access to personal data). A response to a SAR must be issued within 40 calendar days of the date of receipt of the request. However, requests for personal data which can be answered through normal business processes should be dealt with as at present.

On submission of a SAR, the data subject is entitled to:

- be told that personal data about them is being held/is not held
- be given a description of the personal data and the purpose(s) for which the data is being held

- be informed about the people or organisations or the sorts of people or organisations to whom the data may be disclosed
- be told the sources of the data held
- be provided with an intelligible copy of the data in a permanent form.

It should be assumed that the general public does not understand terminology that is unique to the Housing Executive and any such terms should be either avoided or explained in full to the applicant.

The personal data disclosed should normally be that which is held at the time the request is made. However, routine amendments and deletions of data may continue. To this extent, the data given to the requestor may differ from the data that was held at the time the request was received. No non-routine amendments or deletions are permitted, nor should data be tampered with in any way in order to make it acceptable to the applicant.

Some personal data may be exempt from disclosure or legitimately withheld when responding to a SAR (Exemptions)

12.2 Charges

The Act permits a data controller to make a charge for responding to a SAR; subject to a maximum of £10.00. The Housing Executive cannot process a SAR unless the £10 fee has been paid. The preferred method of payment is by cheque made payable to "The Housing Executive". Payment may also be accepted by Postal Order (made payable to "The Housing Executive"), or cash. All payments should be acknowledged by the issue of a receipt (if the payment was made in person by the Data Subject), or by letter confirming receipt of the fee. Subject Access Fees are coded to Fund 39, Account Reference 1029-32195. Normally payment of the fee should accompany the Subject Access Request; however, the effective date of the Subject Access Request will be the date of receipt of the £10 fee if it is later.

Where a Subject Access Request is received without payment of the fee; the Data Subject should be sent a letter acknowledging receipt of the request and advising that the request cannot be processed until payment of the £10 Subject Access Fee is made. A copy of the NIHE leaflet "The Data Protection Act – Your Rights" should also be enclosed;

Data Protection Leaflet

12.3 Time limits for response

The Act permits a maximum 40 calendar days to respond to a SAR.

12.4 Date of receipt of a Subject Access Request

The SAR is treated as received when it arrives with sufficient information and the £10 fee in any NIHE location, whether it is received in a local or central office. Should a written request be given to an officer on site, the date of receipt will be the date the officer receives it.

12.5 Date of clearance of a Subject Access Request

A SAR is cleared when the response is posted to the requestor, or the requestor is notified that it is available for them to view in a local office.

The NIHE must meet the 40 calendar day deadline to comply with the Act. Data Subjects are entitled to complain to the Information Commissioner if this deadline is missed and the Commissioner will treat such breaches seriously under the Sixth Data Protection Principle (Rights of data subjects).

12.6 Request for access to data

The Housing Executive's policy is to make all personal data available to individuals or their legal representatives on request, unless it is covered by a relevant exemption.

A valid SAR will not always take a standard form. The law states that you do not have to respond to a SAR unless you have received it in writing. However, an e-mail is admissible in this context. If a telephone request is received for personal data, you should ask the data subject to put the request in writing. The letter or e-mail does not have to identify itself as a SAR, i.e. it does not have to include the words "subject access" or "Data Protection Act". A simple request for "information you have got on me" is sufficient to be considered a SAR.

Alternatively, a SAR could be a request to have a copy of one particular document.

A data controller is only obliged to respond to a request where the data subject supplies sufficient information to enable the NIHE to identify the:

- person making the request
- information requested.

To enable the Divisional Co-ordinator / business unit to identify the relevant personal data, the data subject may need to provide:

- their surname, previous surname if applicable, and sufficient forenames
- their current address and any previous address if applicable
- a reference number, e.g. National Insurance Number, staff number, pension number or any other suitable identifier
- their date of birth

If the Divisional Co-ordinator has informed the Data Subject of the need for further information, then the NIHE is not obliged to comply with their request until they have supplied that information. However any such request for information must be reasonable and must not be used as a delaying tactic.

The same procedures will apply where the Subject Access Fee did not accompany the information request.

12.7 Confirming identity

The security requirements of the Act impose a clear responsibility on data controllers to ensure that data is not improperly disclosed. It is important therefore that false requests by persons seeking subject access to which they have no right are prevented.

Access will normally only be given to:

- the Data Subject
- someone authorised by the Data Subject (in writing) to receive the data.

It is the responsibility of the Divisional Co-ordinator (or the business unit receiving the request) to establish the identity of the person making a subject access. Where a request is made by e-mail, it is particularly important to confirm the validity of the request and the identity of the person making the request. Such information can, if considered appropriate, be obtained by telephone, so long as whatever questions are asked would provide sufficient confirmation. A signed statement is not necessarily required to provide the necessary confirmation in e-mail requests.

12.8 Repeat requests

The Housing Executive does not have to comply with a request where it has already complied with an identical or similar request by the same individual, unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

In deciding what amounts to a reasonable interval, the following factors should be considered:

- the nature of the data
- the purpose for which the data are processed
- the frequency with which the data are altered.

12.9 Data subject representatives

Disclosure of personal data to data subject representatives should only be made where the consent of the data subject has been given, unless the representative is legally empowered to act on behalf of the data subject.

If you are in any doubt about whether the representative is who they say they are, or whether consent is valid, you should not disclose the data. In all cases a decision must be made on an individual basis.

There are certain representatives who are legally empowered to act on behalf of a data subject:

- a person given Power of Attorney (by a court or by the data subject themselves) deals with all aspects of the data subject's financial affairs. If this is the case you may disclose any data to that representative that could normally be given to the data subject.

Data cannot be disclosed to someone just because they work for a representative group such as CAB or welfare rights groups unless the customer has consented.

Before disclosing data to anyone other than the data subject, you must be satisfied that the representative is:

- who they say they are, and
- either acting with the consent of the data subject or has been appointed by a Government Department or a Court to act for the data subject, and
- asking for relevant information.

12.10 Requests from members of staff/ex-employees

Members of staff/ex-employees of the Housing Executive have the same rights under the Act as members of the general public and data can be held on them both in their capacity as employees and as customers of the Housing Executive.

SARs from employees/ex-employees requesting personnel details should be forwarded to the Divisional Co-ordinator, Personnel & Management Services Division.

12.11 Editing

The reply to a SAR should include all the data that is held on a data subject at the time the SAR is received, without amendment.

There are three exceptions to this rule:

- Normal amendments or deletions can be made to the data after the SAR is received, but before a response is issued. For example, this could take the form of a change of address or bank details. In such cases the previous details may in fact be deleted from the records.
- Data classified as exempt is not disclosed to the data subject
- Other individual's data, including staff names may be withheld in certain circumstances.

The data must never be altered in order to make it acceptable to the data subject.

If during the collection of data for the response, data is identified which contravenes any of the DP Principles, that data must be included in the response but made compliant immediately following it.

12.12 Exemptions

In certain circumstances, personal data does not have to be disclosed to the data subject in response to a SAR. The primary exemptions relate to:

- safeguarding national security
- prevention or detection of crime
- apprehension or prosecution of offenders
- assessment or collection of tax or duty
- personal data concerning physical or mental health
- personal data concerning school pupils
- personal data processed by government departments or local authorities for the purposes of social work
- regulatory functions exercised by public "watchdogs"
- journalistic, literary or artistic purposes
- research, historical and statistical purposes
- where the information is obliged to be made public under enactment

- where disclosure is required by law or made in connection with legal proceedings, etc.
- parliamentary privilege
- where a claim to legal professional privilege could be maintained
- where data is processed only for personal or family affairs.

Further detail on the exemptions can be seen in part 4 (sections 27 to 39) of the

Act; Data Protection Act 1998

The Information Commissioner is critical of organisations that, while withholding data legitimately, do not quote the correct sections of the Act to support their decision. Care must be taken to fully document any decision to block exempt data. In cases where the reason for non-disclosure falls under more than one section of the Act, all relevant sections must be recorded.

Once exempt data has been redacted it may be that there is very little left on the document for the data subject to read. The document must still be issued to the data subject; otherwise the NIHE will be in breach of the Act.

If, when the exempt data is erased or blocked, it is still possible for inference to be drawn from the remaining data, insufficient data has been removed. It should not be possible for anyone to have any understanding of the data which is being withheld.

The fact that information was given to the NIHE in confidence, or a document bears a protective security marking, does not automatically guarantee that the information will be withheld. Privacy markings such as “in confidence” etc. have little effect under the terms of the Act – the disclosability or otherwise of such documents depends on the content, not the endorsement.

12.13 Data relating to another/other individual

Another/other individual’s data means personal data relating to any person other than the:

- data subject
- data controller

Another individual’s data can take two forms:

- data supplied by another individual which relates to the data subject
- details contained in the data of a data subject, which relates to someone other than the data subject.

The rule regarding disclosure of another individual’s data is that the data controller is not obliged to disclose it unless:

- the other individual has consented to the disclosure to the data subject, or
- it is reasonable in all the circumstances to make the disclosure without the consent of the other individual.

The disclosure of another individual’s data may result in a complaint by the other individual or the data subject to the Commissioner if either is unhappy with the decision made. It is

therefore important that all aspects are carefully considered before deciding to release or withhold another individual's data.

Each case should be considered separately. The key questions to ask before deciding whether to disclose the information or not are:

Has the other individual consented to the disclosure?

Consideration should be given to seeking consent. It may not always be appropriate to seek consent, for example if it will mean disclosing data about the data subject to the other individual.

Has the other individual previously given the information to the data subject making the request?

The NIHE would not be justified in withholding the data in these circumstances.

Is the other individual's data confidential, sensitive or harmful to either the other individual or the data subject?

A duty of confidentiality arises in many relationships. When a clear duty of confidentiality to another individual arises, it may not be reasonable to disclose any data, which may identify that other individual; for example in ASB or Harassment cases.

Is it reasonable to disclose the data without the consent of the other individual?

Consideration should be given to disclosing the data without the consent of the other individual: e.g. when an employer has provided wage details. However, if the employer has requested that the source of the data be withheld, consideration will have to be given to withholding their names under section 7(6)(a).

Is the other individual not prepared to consent to the data being divulged to the legal representative of the data subject?

The other individual may be willing to consent to the data subject being given the data, but not the legal representative of the data subject. In such a case, the data relating to the other individual cannot be divulged to the legal representative. It may be appropriate to contact the data subject to advise them of this and if necessary, send the data direct to the data subject.

Has the other individual refused consent to the disclosure?

If the other individual has refused consent to disclosure of the data, then this should be taken as a strong indication that the data should not be disclosed. However, the Commissioner has advised that if consent has not been given, the data controller is still required to release the data if it is reasonable in all the circumstances.

Reasonable is not defined, but if a clear duty of confidentiality arises disclosure of another individual's data without consent is unlikely to be reasonable. The NIHE must consider the circumstances of each case, and make a judgement as to the confidentiality of the data.

Any decision to disclose data without the consent of the other individual must be fully documented.

Does the other individual's data contain details which will identify them? If so, will blocking be sufficient to prevent the disclosure of the other individual?

If it is decided that the other individual's data is to be blocked, disclosure of the remaining data must be made. In this situation, the person blocking the data must be positive that the other individual cannot be identified from what will be disclosed to the data subject.

Information supplied by doctors

Data supplied by doctors can be released to a data subject unless it has been decided it is medically harmful. If it does not contain medically harmful data, normal guidance relating to other individuals should be followed when deciding whether to release the data. In some instances it will be necessary to consult the doctor or other medical practitioner.

Record of reasons for decision

Where it is decided that any information should be withheld and not disclosed to the data subject, the reasons and factors considered which lead to that decision should be recorded.

Enquiries following a response to a Subject Access Request

Enquiries following responses to SARs will normally fall into one of five areas:

- The data subject believes they have not received all the data held on them
- The data subject does not understand the data
- The data subject disputes the accuracy and/or the relevance of the data.
- The data subject finds some of the data offensive.
- The data subject is unhappy that the response was not issued within the timescales allowed.

Each of these is dealt with separately below.

Any of the above may be disputed by the data subject, in the form of an enquiry or a request for a Review. It will be for the Divisional Co-ordinator to decide, if they are the first to receive the correspondence from the data subject, whether it is a formal Review request.

If it is a Review request, then it will be dealt with by the relevant functional director with support from the Records Manager.

The data subject believes they have not received all the data held on them

If the data subject believes they have not received all the data held on them, investigate the claim and reply appropriately.

The data subject does not understand the data

If the data subject does not understand the data, this may be because they do not understand the technical aspect of the data.

Decide, in conjunction with a relevant expert, the most appropriate method of clearing the query.

If the data subject does not understand some of the abbreviations in the text, issue an explanation of the specific abbreviations in question.

If documents are badly written (and therefore unintelligible) issue them together with a typed copy of the text. If a document cannot be deciphered, include an explanation of this in the SAR response.

The data subject disputes the accuracy and/or the relevance of the data

If there is a dispute over the accuracy or relevance of the data, this should be investigated and a decision made as to whether to retain, amend or erase the data.

The reason(s) for the decision should be noted on the file and on any computer system records and the data subject should be notified of the reason(s) for the decision.

If the disputed data is not to be destroyed for whatever reason, for example it is correct, or accepted as incorrect but cannot be altered due to the limitations of the computer system, tell the data subject, and give a written explanation.

Once the disputed data is destroyed through the normal document retention procedures, make sure all references to it are removed from manual and computer records.

The data subject finds some of the data offensive

If the data subject feels some of the data is offensive, always treat this situation as a complaint and refer the matter to the Data Protection Officer, HQ.

The data subject is unhappy that the response was not issued within the timescales allowed

The data subject may be unhappy that the response has not been issued within the 40 calendar day deadline. The response should have included an apology for missing the deadline.

When an enquiry is received following that response, tell the data subject why the deadline was missed. They should also be told that if they are still dissatisfied, they can complain to the Information Commissioner. The address of the Commissioner should be included in the reply

Data subject alleges damage and distress

If a data subject alleges damage (or damage and distress) it can come to the attention of the Data Protection Officer;

- directly from the data subject
- as a result of an allegation made to the Commissioner

If the allegation is received directly from the data subject:

- refer it immediately, with brief details of the points at issue, to the Data Protection Officer, and
- advise the data subject that they will be contacted in due course.

If the allegation is made directly to the Information Commissioner, the Data Protection Officer will contact the relevant business manager for details of the case. The request must be replied to immediately.

The Data Protection Officer will:

- formally acknowledge receipt of the allegation to the data subject
- if necessary establish the precise nature of the allegation
- liaise with the Information Commissioner
- alert Legal Department to the possibility of litigation
- advise the business manager of the result of the allegation.

Providing the data in permanent form

You must provide the data of which the applicant is the subject in permanent form unless this is not possible, would involve disproportionate effort or the data subject has agreed to accept the data in another format. Unless there is a good reason not to, you should supply paper copies. You may provide microfilm, audiotapes, videotapes or floppy disks containing the data if the data subject agrees to this, or reasonably requests this. For example, you might provide a blind person with the data in audiotape form or in Braille. Generally speaking you should not read the data out over the phone as this is not a permanent form. If further advice required, contact the Data Protection Officer.

If, after consulting the Data Protection Officer, it is decided that a permanent copy cannot be supplied, the data must still be provided in a non-permanent form.

12.15 Initial action on receipt of a Subject Access Request

A SAR can be received in any part of the NIHE. The person who receives the SAR must contact the relevant Divisional Co-ordinator to advise them that a SAR has been received. It must be faxed, emailed or posted immediately to the Divisional Co-ordinator. The request should be copied to the Records Manager who will open a case folder in Meridio and allocate the request to the appropriate Divisional Rep.

Make sure all SARs are stamped with the date of receipt in the appropriate NIHE office.

12.16 Request by data subject to view/collect data at a NIHE office

The data subject can request that they view/collect their data from any NIHE office.

The Divisional Rep will make the necessary arrangements with the appropriate local business manager for the area in which the data subject wishes to view/collect the data.

Data subjects must always be accompanied when viewing original documents.

Ownership of the Subject Access Request

When a SAR is received, it should be forwarded to the appropriate Divisional Rep on the day of receipt or as soon as possible thereafter.

The Divisional Rep is responsible for:

- Confirming the identity of the data subject (if necessary)
- Confirming that the location of the information requested can be identified
- Ensuring all necessary information is received before responding to the SAR
- ensuring that the £10 Subject Access Fee has been paid
- Registering the request in the SAR Register (see Annex 4)
- Ensuring all action is taken in a timely manner
- Monitoring and controlling the progress of their own actions
- Ensuring all responses are issued to the data subject within the 40 calendar day deadline
- Responding to certain enquiries from the data subject following the issue of the response
- Ensuring all actions have been fully documented in relation to the SAR including filing a scanned copy of the signed decision letter in the Meridio case folder

Insufficient identity details provided by data subject

The Divisional Rep is not obliged to respond to a SAR until all the necessary information to enable the identity check to be carried out is provided. When further information is required, the effective date does not apply, and the 40 calendar day clearance time has not begun. If there are insufficient details, this is referred to as a potential SAR.

The Divisional Rep should contact the data subject, requesting the necessary information, and set a prompt of 30 calendar days, for receipt of the reply from the data subject.

If at the end of the 30 days no reply has been received from the data subject, issue him/her a letter explaining that since there had been no reply to our original request, we will be assuming that they do not wish to proceed with their request and we will be taking no further action.

Retain the SAR file for one calendar month from date of issue of final letter and then destroy it as confidential waste.

Sufficient identity details provided by data subject

Make sure the correct effective date is entered in the file or register, as that will be the date from which the 40 calendar day time limit is calculated from.

If however, the SAR was originally treated as a potential SAR prior to this, the effective date will be the date all the necessary information is received in writing.

If, on initial receipt, the SAR contained all the necessary information to enable the Divisional Rep to deal with it, but was not passed to him/her immediately, this will not alter the overall 40 calendar day time limit.

Payment of the Subject Access Fee after receipt of the request

The effective date of receipt of the Subject Access Request for purposes of the 40 day calculation will be the date on which the Subject Access Fee is received if later than the original request.

Withdrawal of request for access by the data subject

There may be occasions where the data subject may withdraw the SAR, after it has been recorded in the SAR file or log.

The details of the withdrawal should be recorded in the SAR file or register.

The withdrawal of the SAR should be acknowledged in writing. Once this action has been completed, the SAR should be taken as cleared.

Requesting and monitoring requests for records

A data subject may request data from any or all of the following:

- Manual records
- Information held on computer including e-mail
- Close Circuit Television (CCTV)
- taped conservations or their transcripts
- still photographs
- video recordings
- any other media.

Request for data held on Close Circuit Television or audiotape

Should a data subject request data from either CCTV or taped Conservations; seek advice from the administrator of the CCTV system (usually the local office manager where the CCTV is sited).

12. 17 E-Mail

E-mails, both incoming and outgoing, are covered by the Act if one or other of the following criteria is met:

- the sender or recipient is identifiable, either through their e-mail address or the text of the e-mail; or
- the text of the e-mail contains personal data, i.e. facts, opinions or intentions about identifiable living individuals.

Under the Act e-mails in personal mailboxes and deleted items boxes, e-mails saved into Meridio and e-mails placed on paper files that fall within the definition of a relevant filing system are liable for disclosure in response to a SAR. Copies of deleted emails held on back-up systems may also be liable for disclosure.

Blocking exempt or other individuals data

When blocking exempt or other third party data, the Divisional Rep must:

- separate those records which can and cannot be issued to the data subject
- arrange to have all the records which can be issued to the data subject photocopied
- ensure no deletions/amendments are made on original documents
- block any exempt data or other individuals data on the photocopies using a black permanent marker on both sides of the paper if necessary
- arrange records in date order.

Decisions made by the Divisional Rep to withhold data must be fully documented in the SAR file.

Potentially offensive data

The Divisional Rep should, if they believe there is potentially offensive material included in the data which must be issued to the data subject, decide how the situation should be dealt with, e.g. consider an office interview or home visit, instead of posting the data out. Make sure the data subject understands that action is being taken to make the data compliant with the Act.

Whatever the decision, the data must be made compliant, but only after issuing it to the data subject.

Consider the action required to ensure future data is recorded correctly, e.g. referral to the line manager of the staff member concerned.

Inform relevant business manager about the imminent release of potentially offensive data.

12.18 Divisional Rep action before issuing response to Subject Access Request

On receipt of each component, ensure that:

- all data relates to the data subject
- the correct procedures for blocking exempt data are followed
- the correct procedures are carried out in relation to other individuals data
- examine them for potentially offensive data
- NIHE specific abbreviations have been explained
- data which cannot be understood, e.g. because of poor handwriting, must be typed and a copy of the original document issued together with the typewritten transcript. If any part of the document is unreadable, this should be explained to the data subject and an apology included in the reply
- if the latest address on any computer system differs from that on the SAR, verification of the new address is recorded
- arrange copying of all relevant records for issue, which includes any jacket/file cover.

Ensure that the SAR file and register log is updated with relevant information at the appropriate time. This is to ensure that: if any action has not been carried out correctly, there will be a minimum delay in rectifying the situation

Prepare a covering letter to respond to the SAR. This will accompany the data you intend to release or not release. The letter should cover the following areas as appropriate to the particular SAR:

- a description of the personal data of which they are the data subject
- a description of the purposes for processing the data
- information about the people or organisations, or the sorts of people or organisations to whom you might disclose the personal data
- information on the sources of the personal data
- if no data has been found, indicate this to the data subject, or if none of the data can be released, state that there is no data you are required to give.
- an explanation of any inaccurate data being issued and details of the action the NIHE intends to take to correct the problem
- your contact details.

12.19 Final action

Complete the SAR file or log and authorise the release of the response to the data subject. Scan and file a copy of the final letter in the Meridio case folder.

Make sure the letter and any envelopes are addressed correctly to the data subject.

Method of response to the data subject

The data subject may indicate at any time that they would like to:

- have their response posted to them
- view or collect their response personally at a NIHE office.

If they do not express a preference, send the response by post.

Response to be viewed/collected at a NIHE office

Arrangements should already be in place if the data subject has asked to view the records at an office other than that of the Divisional Co-ordinator. When the records are to be viewed at another office, the response, which will be accompanied by the originals if necessary, should be forwarded to the contact point in the office concerned. This is to ensure the data is available for the appointment.

Contact the data subject, if possible by telephone, to arrange a time for them to call. If this is not possible write to the data subject, asking them to contact the Divisional Rep to arrange a time. Record action taken in the SAR file and set an appropriate prompt date for a reply.

The appointment time and date should be arranged in conjunction with the data subject and a senior officer in the office where the records will be viewed.

If there has been no reply to the letter by the time the prompt matures, consider issuing a copy by post.

When the request is to view the originals, the data subject may request a copy of the data at the interview. This should be arranged and the copy issued by post.

Data subject fails to attend the appointment

If the data subject fails to attend the appointment, the Divisional Rep should attempt to contact him or her and make another appointment. If they cannot be contacted, issue the response by post. If another appointment has been arranged and the data subject again fails to attend, issue the response by post.

If it is not possible to issue the response by post, e.g. the person is of no fixed abode, the data should be retained at the office of interview for one month from the date the Divisional Rep tries to contact the data subject, and then destroyed. When originals have been sent to a NIHE office for viewing, return them to the originating office.

Data exists but cannot be found

If it is known that data exists but cannot be found, the Divisional Rep must ensure the business area involved acts in a timely manner in attempting to trace missing documents.

If some data has been traced, continue normal action on that data.

If by the day before the 40 calendar day deadline, it is obvious that the missing data will not be found in time, then the data held by the Divisional Rep should be issued to the data subject.

A letter should be issued to the data subject explaining what data has been found and apologising, as the full response has not been issued within the 40 calendar days, and the NIHE has failed to meet the deadline.

When the missing action is completed and data has been traced, it should be issued to the data subject with an explanatory letter.

If, following a search for a missing document, the data cannot be traced, the SAR file should be updated and a suitable explanatory letter should be issued to the data subject.

Data should exist but has been destroyed in error

If the Divisional Rep is aware that data should exist for the data subject but has proof that it has been destroyed in error, the Divisional Rep should write to the data subject, explaining the situation and apologising for the error.

The deadline will have been met if it is established within the 40 calendar day deadline that the data has been accidentally destroyed and either:

- that was all the data requested, or
- the other data requested had been issued within the 40 calendar days.

No data held for a data subject

It may be that a Business Area/Unit from which the data subject has requested data does not hold anything for the data subject.

In such a case the Divisional Rep Officer should enter this in the SAR file and issue the data subject with an appropriate letter. This will advise the data subject that their SAR has been dealt with and there are no records held for them.

13.0 THIRD PARTY ACCESS TO PERSONAL DATA

This section explains that written requests should be handled as set out in the FOI Procedures Manual

13.1 There is no right of access to information about other people (3rd parties) in the Data Protection Act. However, the Freedom of Information Act provides a limited right of access to this information – limited by the need to comply with the Data Protection Principles and generally be fair to data subjects. See the FOI Procedures Manual for how to handle requests by 3rd parties, which must be in writing. Standard letters and paragraphs to be used in replies are annexed to those procedures and must be used.

13.2 However, common sense can be applied here. If someone telephones to ask for the name of a member of staff with a particular work responsibility because they have a business reason for contacting them, provide the name and business contact details unless there is a particular reason not to do so.

If you have any doubts, take the caller's contact details and say that you will ask the staff member concerned to contact them. Never provide a home address or phone number.

14.0 SENDING PERSONAL DATA OUT OF THE COUNTRY

This section provides alerts to problems with exporting personal information.

14.1 Except in response to a Subject Access Request, do not transfer personal information about living individuals outside the European Economic Area (EU countries, Iceland, Liechtenstein and Norway) unless (i) the data subject has given consent or (ii) a contract is in place which provides equivalent protection of the rights of data subjects. For more information on the countries to which personal information can be exported, see:

Information Commissioner's Office

14.2 Transfer means physically transporting the data overseas as well as providing people abroad with access to the information, for example, via the internet. We will not place on our website personal information about staff, other than names, email addresses and, in some circumstances, work responsibilities, without their consent.

15.0 FURTHER INFORMATION AND ADVICE

For further advice contact the Data Protection Officer / Records Manager, on extension 2970, or the Legal Department.