Pentland Housing Group

Document Type	Policy
No	C12
Name	Data Protection Policy
Group	Pentland Housing Association Ltd Pentland Community Enterprises
Type	Corporate
Lead Body	Audit Committee
Lead Officer	Corporate Officer
Version	5
Original Authorisation by PHA Board	October 2002
Previous Authorised by PHA Board	October 2012
Latest Authorised by PHA Board	13 January 2016
Review Due Date	January 2019
Reviewed by Audit Committee	28 October 2015
Consultation	Management Team – 8 September 2015 PCE – 25 November 2015
Electronic Storage	N:\PHA\Corporate\Policies & Procedures\Corporate
Website	
Secure Area of Website	

Pentland Housing Group

Data Protection Policy

1 General Information

1.1 The PHA Group is committed to protecting the rights and privacy of individuals in accordance with the Data Protection Act 1998. The Group processes information about its staff, tenants and other individuals it has dealings with for a range of administrative purposes (eg 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.

1.2 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.

1.3 Under the 1998 Act, all organisations that process personal information are required to notify the Information Commissioner's Office. The Group'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 Group's notification can be found at http://www.informationcommissioner.gov.uk/ - the registration number is Z6087563.

1.4 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/.

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

1.6 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 – ie data which is incorrect or misleading

1.7 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).

1.8 You are specifically cautioned that the PHA Group does not authorise any employee or agent of the Group to hold or process any personal data on its behalf except as stated in the Group's Notification. Users of personal data within or out with the Groups Office (eg pc at home or laptop) should consider the legal position before attempting to process personal data.

1.9 In cases of doubt or difficulty staff should in the first instance contact the Group Chief Executive.

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

2 Section 1: Policy Statement

2.1 The PHA Group 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 Group 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.

2.2 The policy applies to all staff of the Group. Any breach of the Data Protection Act 1998 or the Group Data Protection Policy is considered to be an offence and in that event, the PHA disciplinary procedures will apply. As a matter of good practice, other agencies and individuals working with the Group, 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.

3 Section 2: Background to the Data Protection Act 1998

3.1 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.

4 Section 3: Definitions (Data Protection Act 1998)

4.1 Data - Data means information which

(a) Is being processed on a computer, or intended to be held on a computer by means of equipment operating automatically in response to instructions given for that purpose,
(b) Is recorded on a computer, or intended to be held on a computer with the intention that it should be processed by means of such equipment,
(c) Is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) Does not fall within paragraph (a), (b) or (c) but forms part of an accessible record defined by Section 68 of the Data Protection Act 1998, or
(e) Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

4.2 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.

4.2 **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.

4.3 **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.

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

4.5 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.

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

4.7 **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.

4.8 **Tenant -** The term "tenant" (meaning a tenant of the Group) 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 Pentland Housing Group.

5 Section 4: Responsibilities under the Data Protection Act

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

6 Section 5: Notification

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

7 Section 6: Data Protection Principles

7.1 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 and, in particular, shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met. .
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
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
8. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless the 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.

8 Section 7: Data Subject Rights

8.1 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.

9 Section 8: Consent

9.1 Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. The Group 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.

9.2 In most instances consent to process personal and sensitive data is obtained routinely by the Group (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 of The Group's 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.

9.3 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.

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

10 Section 9: Security of Data

10.1 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).

10.2 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

10.3 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.

10.4 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.

10.5 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 the Groups offices.

11 Section 10: Rights of Access to Data

11.1 Members of the Group have the right to access any personal data which are held by the Group 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 Group about that person.

11.2 Any individual who wishes to exercise this right should apply in writing to the Chief Executive. The Group 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.

11.3 In order to respond efficiently to subject access requests the Group needs to have in place appropriate records management practices. See the Group's Document Retention of Archives Policy.

12 Section 11: Disclosure of Data

12.1 The Group 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 Group 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 Group concerned.

12.2 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 Group corresponding with a named third party);
2. where the disclosure is in the legitimate interests of the Group (eg disclosure to staff - personal information can be disclosed to other Group employees if it is clear that those members of staff require the information to enable them to perform their jobs);
3. where the Group 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.

12.3 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.

12.4 When members of staff receive enquiries as to whether a named individual is a member of the Group, 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 Group may constitute an unauthorised disclosure.

12.5 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.

12.6 As an alternative to disclosing personal data, the Group 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.

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

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

12.9 If in doubt, staff should seek advice from their Head of Department or the Chief Executive.

13 Section 12: Retention and Disposal of Data

13.1 The Group 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 Group, it will not be necessary to retain all the information held on them. Some data will be kept for longer periods than others.

13.2 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 in accordance with the Group's Document Retention of Archives Policy.

13.3 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. Other information relating to individual members of staff will be kept according to the Document Retention of Archives Policy.

Information relating to unsuccessful applicants in connection with recruitment to a post must be kept for 12 months from the interview date. The Group 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.

13.4 Disposal of Records

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

14 Section 13: Publication of Group Information

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

- Information published in the Groups Corporate Diary/Outlook system
- Names of all members of Group’s Board of Directors
- Names and job titles of staff.
- Internal Telephone Directory.
- Information in publications (including photographs), annual reports, newsletters, etc.

- Staff information on the Group 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 Group should comply with the request and ensure that appropriate action is taken.

15 Section 14: Direct Marketing

15.1 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 (e.g. an opt-out box on a form).

16 Section 15: Academic Research

16.1 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.

16.2 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

16.3 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 made anonymous (exemption from part of Principle 6 relating to access to personal data).

16.4 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.

16.5 Notes to Researchers

Whilst the Act states that research may legitimately involve processing of personal data beyond the originally stated purposes (e.g. longitudinal studies), the Group 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.

16.6 Publication

Researchers should ensure that the results of the research are made anonymous 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.

Version 1	October 2002
Version 2	
Version 3	
Version 4	October 2012
Version 5	January 2016