VHA Policy Document

DATA PROTECTION POLICY

Reviewed: June 2015

Next Review Due: June 2018

VHA Data Protection Policy

1.0 INTRODUCTION

1.1 As a landlord and employer, VHA holds personal information on a variety of people, including customers (current, former and prospective), current and former employees, job applicants, and contractors. VHA is committed to protecting the rights of individuals' privacy with regard to the processing of personal data. We demonstrate this through operating within the requirements of the Data Protection Act 1998 with regards to collecting, storing, divulging, sharing and disposing of personal information.

2.0 BACKGROUND AND CONTEXT

2.1 The Eight Principles of Data Protection are outlined in the Act, and are enforceable by law.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

2.2 The organisation and all staff who process any personal information about other people must ensure that they comply with this Data Protection Policy.

3.0 PURPOSE AND SCOPE OF THE POLICY

3.1. Purpose

VHA is committed to protecting the rights and privacy of individuals (includes staff, customers and others) in accordance with the General Data Protection Regulations and the Data Protection Act ("the Act") to which it is subject as a controller and processor of personal data ("data controller"). VHA needs to process information about its staff, customers and other individuals ("data subjects"), to run our business - for example, to allocate properties, manage customers' tenancies, recruit and pay staff, monitor performance and customer feedback. Such information must be collected and used fairly, stored safely and not disclosed unlawfully.

3.2 Scope

The policy covers the processing of personal data whose use is controlled by VHA Housing Association and defined in the organisation's Data Protection Notification:

VHA HOUSING ASSOCIATION LTD ref 5740272

Personal data is interpreted as information relating to an identifiable individual, usually held in one of four types:

(i) information processed, or intended to be processed, wholly or partly by automatic means (that is, information in electronic form usually on computer) ;
(ii) information processed in a non-automated manner which forms part of, or is intended to form part of, a 'filing system' (that is usually paper records in a filing system)
(iii) information that forms part of an 'accessible record' (that is, certain health records, educational records and certain local authority housing or social services records, regardless of whether the information is processed automatically or is held in a relevant filing system) ; and
(iv) information held by a public authority (referred to as 'category 'e' data' as it falls within paragraph (e) of section 1(1) of the DPA).

It applies to all staff, contractors and consultants who process data on behalf of the organisation. Personal data applies to both computer and manual records. Any breach of the Act or failure to follow this Data Protection Policy may therefore result in disciplinary proceedings.

3.3 .Responsible Authorities

VHA is the 'data controller' under the Act. All those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the organisation. Compliance with this Data Protection Policy is the responsibility of all staff. The ultimate responsibility to ensure VHA compliance rests with the Chief Executive.

4.0 KEY PRINCIPLES

4.1 VHA is committed to working according to the Eight Principles of Data Protection (see section 2), and will apply these in the following areas:

- Data Security
- Rights of Data Subjects
- Rights to Access Information
- Disclosure of Data
- Retention and Disposal of Data

5.0 DATA PROTECTION POLICY

5.1 Data Security

All users of personal information provided by VHA are responsible for ensuring that any personal information that they hold about other people:

1. Is kept securely. For paper records, this means being kept in a lockable room with controlled access, or kept in a locked drawer or filing cabinet. For computerised records, this means ensuring they are password protected, and kept on disks which are themselves stored securely
2. Is not disclosed in any form to any unauthorised third party.

Unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct.

5.1.1 Use of IT

Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that passwords are kept confidential. Logged-In PCs should not be left unattended without logging out or using a password protected screen saver.

Staff are not permitted to send attachments containing the personal details of customers or colleagues to external email addresses, unless we have formal data sharing arrangements with the recipient organisation. This includes a prohibition on sending personal details to staff members' own personal email accounts

All staff will have encrypted memory sticks issued to them. Any VHA information required to be saved and taken externally should only be saved on such devices.

Any staff leaving VHA will have their accounts disabled immediately.

Managers are not to access team members' email accounts except in cases of suspected fraud

5.1.2 Home / mobile working

When working from home, staff should:

- Not save any VHA documents on personal computers or laptops, or on personal memory sticks

When mobile working, staff should

- Work exclusively on the network, and not save documents to the hard drive of the computer they are using
- not store the login / password information with the laptop they relate to

5.1.1 Staff records

Staff are responsible for:

- Ensuring that any personal data supplied to VHA is accurate and up-to-date;
- Informing their manager of any changes to information that they have provided about themselves e.g. changes of address.

Managers should not hold personal details of staff members in their drawers - this should all be held in secure cabinets. Staff who want to access their own information, or managers who wish to access that of their staff, should contact their manager or the Chief Executive.

A member of staff who considers this Data Protection Policy has not been followed in respect of personal data about himself/herself should first raise the matter with their line manager, who will in turn raise the issue with the Chief Executive.

5.2 Rights of Data Subjects

All data subjects are entitled :

- to know what information VHA holds and processes about them and why;
- to gain access to it;
- to keep it up to date;
- to require the organisation to rectify, block, erase or destroy inaccurate information;
- to prevent processing likely to cause unwarranted damage or distress;
- to prevent processing for the purposes of direct marketing;

- to compensation where a data subject suffers damage, or damage and distress, as a result of a breach of the Act.

5.3 Rights to Access Information

Data subjects have the right to access personal information kept about them by VHA, both in electronic and paper files.

For data subjects wanting access to their information, a subject access request should be made in writing to the Deputy Chief Executive. VHA will make a charge of £10 on each occasion that such access is requested.

The data subject will receive access within 40 days of receipt of a written request, the fee and any information necessary to satisfy the organisation as to the identity of the person making the request.

Staff wanting access to their personnel file should request this through the Chief Executive. The information will be provided within 10 working days.

5.4 Disclosure of Data

VHA must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, external organisations and partner agencies. All staff should exercise caution when asked to disclose personal data held on another individual to a third party.

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

- the individual has given their consent (e.g. a customer/member of staff has consented to VHA corresponding with a named third party);
- where the disclosure is in the legitimate interests of the institution (e.g. disclosure to staff - personal information can be disclosed to other employees if it is clear that those members of staff require the information to enable them to perform their jobs);
- where VHA is legally obliged to disclose the data

Permission to disclose customers' personal details to contractors will be taken at sign up. Contractors will be required to comply with VHA's Data Protection Policy in the disposal of their duties.

5.5 Retention and Disposal of Data

The Act forbids the retention of personal data for longer than it is required. Once customers are no longer tenants / leaseholders of VHA, or once staff have left employment, it will not

be necessary to retain all the information held on them. Some data will be kept for longer periods than others. VHA will follow the guidance as set out in the National Housing Federation Document Retention Schedule. A summary of the main impact on customers and staff is outlined below:

Customers

For most former tenants, we will hold electronic details of them and their tenancy for 3 years. We will keep details on former tenants who are in rent arrears for as long as we are pursuing the arrears. We will retain indefinitely a copy of the tenancy agreement for all former tenants.

Staff

All information about staff will be kept for six years after their employment ceases.

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

All other documents will be retained for periods as outlined in the NHF good practice guidance.

Disposal of Records

Appropriate security measures are in place for the deletion or disposal of personal data.

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).

Senior managers should ensure review archives on a six monthly basis to dispose of documents. A secure shredding service will be used.

Responsibility for establishing disposal mechanisms for documents in their areas of the business lies with the relevant senior manager.

6.0 CUSTOMER IMPACT

6.1 All customers, as data subjects, are protected by this Policy. They will be provided with reassurance that their privacy is being protected, and have clear procedures for requesting access to their information.

7.0 REVIEWING THE POLICY

7.1 This policy will be reviewed on a tri- annual basis, or when change in the law necessitates an immediate review. The next review date is therefore May 2018.