Scottish Veterans Residences

DATA PROTECTION POLICY

Contents

1. Introduction

Scottish Veterans Residences (hereinafter the "Association") is committed to ensuring the secure and safe management of data held by the Association in relation to residents, staff and other individuals. The Association's staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

The Association needs to gather and use certain information about individuals. These can include residents and tenants, employees and other individuals that the Association has a relationship with. The Association manages a significant amount of data, from a variety of sources. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the GDPR).

This Policy sets out the Association's duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.

Appendix 1 hereto details the Association's related policies.

2. Legislation

It is a legal requirement that the Association process data correctly; the Association must collect, handle and store personal information in accordance with the relevant legislation. This policy sets our commitment to protecting personal data and how we will implement this with regards to the collection and handling of personal data as defined in the following legislation:

(a) the General Data Protection Regulation (EU) 2016/679 ("the GDPR");

(b) UK Data Protection Act 2018 (DPA2018)

(c) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and

(d) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union.

Failure to comply with data protection legislation could lead to financial penalties, regulatory action, as well as reputational damage.

3. Scope

The Policy applies to all personal data that the Association holds relating to living identifiable individuals regardless of the category of data or the format of the data. Personal data is any data which could be used to identify a living individual e.g. name, address, email, postcode, CCTV image, and photograph. Special categories of personal data is any information about racial or ethnic origin, political opinions, religious beliefs, health (mental and physical), sexual health, trade union membership and criminal convictions.

The policy applies to personal data held or accessed on the Association's premises or accessed remotely via home or mobile working. Personal data stored on personal and removable devices are also covered by this policy.

This policy applies to:

- All Staff, including temporary staff
- Volunteers
- Members of the Governing Body

The Data Protection Principles

Data protection laws describe how organisations must collect, handle and store all personal data. Ensuring compliance is underpinned by the following principles.

Personal data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay;

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition to these principles the law requires organisations to be responsible for, and must be able to demonstrate, compliance with the above principles.

Responsibilities for Compliance

The Governing Body is ultimately responsible for ensuring that the Association meets its legal obligations.

All staff, volunteers, Governing Body members have a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in line with this policy and the data protection principles.

The Head of External Relations is responsible for monitoring compliance with this policy and the data protection legislation; managing personal data breaches and data subject rights; recording and maintaining appropriate records of processing activities and the documented evidence required for compliance.

Compliance

The Association will comply with our legal obligations and the data protection principles by:

<u>Processing Lawfully and Fairly</u>
The Association will ensure processing of personal data, and special categories, meets the legal basis as outlined in legislation. Individuals will be advised on reasons for processing via a freely available Fair Processsing Notice (FPN).

Where data subjects' consent is required to process personal data, consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the process for Data Subjects to withdraw consent will be simple.

Purposes
Personal data will only be used for the original purpose it was collected for. These purposes will be clear to the data subject.

If the Association wish to use personal data for a different purpose, we will notify the data subject prior to processing.

Adequate and Relevant data
The Association will only collect the minimum personal data required for the purpose. Any personal data discovered as excessive or no longer required for the purposes collected for will be securely deleted.

Any personal information that is optional for individuals to provide will be clearly marked as optional on any forms.

Accurate
The Association will take reasonable steps to keep personal data up to date, where relevant, to ensure accuracy.

Any personal data found to be inaccurate will be updated promptly. Any inaccurate personal data that has been shared with third parties will also be updated.

Retention
The Association will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data are outlined in the Records Retention Schedule.

Data will be disposed of in a responsible way to ensure confidentiality and security.

4. Data

4.1 The Association holds a variety of Data relating to individuals, including residents, tenants and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by the Association is detailed within the Fair Processing Notice at Appendix 2 hereto and the Data Protection Addendum of the Terms of and Conditions of Employment which has been provided to all employees.

4.1.1 "Personal Data" is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by the Association.

4.1.2 The Association also holds Personal data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

5. Processing of Personal Data

5.1 The Association is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject (see clause 4.4 hereof);
- Processing is necessary for the performance of a contract between the Association and the data subject or for entering into a contract with the data subject;
- Processing is necessary for the Association's compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the data subject or another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the Association's official authority; or
- Processing is necessary for the purposes of legitimate interests.

5.2 Fair Processing Notice

5.2.1 The Association has produced a Fair Processing Notice (FPN) which it is required to provide to all residents or tenants whose Personal data is held by the Association. That FPN must be provided to the client from the outset of processing their Personal Data and they should be advised of the terms of the FPN when it is provided to them.

5.2.2 The Fair Processing Notice at Appendix 2 sets out the Personal Data processed by the Association and the basis for that Processing. This document is provided to all of the Association's clients at the outset of processing their data.

5.3 Employees

5.3.1 Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Association. Details of the data held and processing of that data is contained within the Employee Fair Processing Notice which is provided to Employees at the same time as their Contract of Employment.

5.3.2 A copy of any employee's Personal Data held by the Association is available upon written request by that employee from the Association's Company Secretary.

5.4 Consent

Consent as a ground of processing will require to be used from time to time by the Association when processing Personal Data. It should be used by the Association where no other alternative ground for processing is available. In the event that the Association requires to obtain consent to process a data subject's Personal Data, it shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by the Association must be for a specific and defined purpose, eg, to accept electronic marketing material, (i.e. general consent cannot be sought).

5.5 Processing of Special Category Personal Data or Sensitive Personal Data

In the event that the Association processes Special Category Personal Data or Sensitive Personal Data, the Association must do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose;

- Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity; and
- Processing is necessary for reasons of substantial public interest.

6. Data Sharing

In certain circumstances the Association may share personal data with third parties. This may be part of a regular exchange of data, one-off disclosures, or in unexpected or emergency situations.

Appropriate security measures will be used when sharing any personal data.

Where data is shared regularly a contract or data sharing agreement will be in place to establish what data will be shared and the agreed purpose.

The Association will consider all the legal implications of sharing personal data prior to doing so.

Data Subjects will be advised of any data sharing in the Privacy Notice.

6.1 The Association shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with the Association's relevant policies and procedures. In order that the Association can monitor compliance by these third parties with Data Protection laws, the Association will require the third party organisations to enter in to an Agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches.

6.1..1 Personal data is from time to time shared amongst the Association and third parties who require to process personal data that the Association process as well. Both the Association and the third party will be processing that data in their individual capacities as data controllers.

6.1..2 Where the Association shares in the processing of personal data with a third party organisation which is a separate or joint Data Controller (e.g. for processing of the employees' pension), it shall require the third party organisation to enter in to a Data Sharing Agreement with the Association in accordance with the terms of the model Data Sharing Agreement set out in Appendix 3 to this Policy.

6.2 Data Processors

A data processor is a third party entity that processes personal data on behalf of the Association, is under a contract to provide a service to the Association and is engaged if certain of the Association's work is outsourced (e.g. payroll, maintenance and repair works).

6.2.1 A data processor must comply with Data Protection laws. The Association's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the Association if a data breach is suffered.

6.2.2 If a data processor wishes to sub-contract their processing, prior written consent of the Association must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

6.2.3 Where the Association contracts with a third party to process personal data held by the Association, it shall require the third party to enter in to a Data Protection Addendum with the Association in accordance with the terms of the model Data Protection Addendum set out in Appendix 4 to this Policy.

7. Data Storage and Security

All Personal Data held by the Association must be stored securely, whether electronically or in paper format.

7.1 Paper Storage

If Personal Data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no Personal Data is left where unauthorised personnel can access it. When the Personal Data is no longer required it must be disposed of by the employee so as to ensure its destruction. If the Personal Data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored in accordance with the Association's storage provisions.

7.2 Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to the Association's data processors or those with whom the Association has entered in to a Data Sharing Agreement. If Personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drives and servers.

8. Breaches

Security Incident & Breach Management

Occasionally the Association may experience a personal data breach; this could be if personal data is:

- Lost, for example via misplacing documents or equipment that contain personal data, through human error, or via fire, flood or other damage to premises where data is stored
- Stolen; theft or a result of a targeted attack on our network (cyber-attack)
- Accidently disclosed to an unauthorised individual
- Inappropriately accessed or used

All security incidents or personal data breaches will be reported and managed by the Head of External Relations.

The Information Commissioner's Office and the individuals affected will be notified promptly, if required.

All breaches will be managed under the Association's Breach Management Procedures as follows:

8.1 A data breach can occur at any point when handling Personal Data and the Association has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally in accordance with Clause 7.3 hereof.

8.82 Internal Reporting

The Association takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Head of External Relations must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- The Association must seek to contain the breach by whatever means available;
- The Head of External Relations (with advice from the Data Protection Officer, where appropriate) must consider whether the breach is one which requires to be reported to the ICO and data subjects affected and do so in accordance with this clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements
- The Company Secretary is be informed of a data breach and act as above in the absence of the Head of External Relations.

8.3 Reporting to the ICO

If the Head of External Relations considers the breach may result in a high risk to the rights and freedoms of the data subject, the Data Protection Officer must be informed.

The Data Protection Officer will give advice and recommend whether it is appropriate to report the breach to the Information Commissioner's Office ("ICO") and/or the Data Subject(s) affected.

If the decision is made by the Association to report the breach to the ICO this must be done by the Data Protection Officer within 72 hours of the Association becoming aware of the breach having occurred.

9. Data Protection Officer ("DPO")

9.1. A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by the Association with Data Protection laws. The Association has appointed RGDP LLP as their Data Protection Officer; whose details are noted on the Association's website and contained within the Fair Processing Notice at Appendix 3 hereto.

9.2 The DPO will be responsible for:

9.2.1 monitoring the Association's compliance with Data Protection laws and this Policy;

9.2.2 co-operating with and serving as the Association's contact for discussions with the ICO

9.2.3 reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

10. Data Subject Rights

Certain rights are provided to data subjects under the GDPR. The Association will uphold the rights of data subjects to access and retain control over their personal data held by us.

The Association will comply with individuals':

- **Right to be Informed** – by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.
- **Right to Access** – by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.
- **Right to Rectification** – by correcting personal data that is found to be inaccurate. We will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies with be rectified without undue delay.
- **Right to Erasure** (also known as 'the right to be forgotten') - we will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.
- **Rights to Restrict Processing** - we will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right.
- **Right to Data Portability** – by allowing, where possible, data to be transferred to similar organisation in a machine-readable format.
- **Right to Object** – by stopping processing personal data, unless we can demonstrate legitimate grounds for the processing, which override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defence of legal claims.

Not all of the above rights apply in all circumstances. Which rights do apply depends on the purpose for which the personal data is being processed by the Association.

10.1. Subject Access Requests

Data Subjects are permitted to view their data held by the Association upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, the Association must respond to the Subject Access Request within one calendar month of the date of receipt of the request. The Association:

10.1..1 must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law.

10.1..2 where the personal data comprises data relating to other data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request, or

10.1..3 where the Association does not hold the personal data sought by the data subject, must confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

10.2 **The Right to be Forgotten**

10.2..1 A data subject can exercise their right to be forgotten by submitting a request in writing to the Association seeking that the Association erase the data subject's Personal Data in its entirety.

10.2..2 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The Head of External Relations (with advice from the DPO, where appropriate) will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.4 and will respond in writing to the request.

10.3 **The Right to Restrict or Object to Processing**

10.3.1 A data subject may request that the Association restrict its processing of the data subject's Personal Data, or object to the processing of that data.

10.3.1.1 In the event that any direct marketing is undertaken from time to time by the Association, a data subject has an absolute right to object to processing of this nature by the Association, and if the Association receives a written request to cease processing for this purpose, then it must do so immediately.

10.3.2 Each request received by the Association will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The Head of External Relations (with advice from the DPO, where appropriate) will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.5 and will respond in writing to the request.

11. Privacy by Design

11.1 The Association has an obligation to implement technical and organisational measures to demonstrate that we have considered and integrated data protection into our processing activities throughout the organisation.

11.2 When introducing any new type of processing, particularly using new technologies, we will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and carry out a Data Protection Impact Assessment.

11.3 All new policies including the processing of personal data will be reviewed by the Head of External Relations to ensure compliance with the law and establish if a Data Protection Impact Assessment is required.

11.4 Advice will be provided by the Data Protection Officer on conducting Data Protection Impact Assessments in line with the Association's Data Protection Impact Assessment Procedure.

12. Data Protection Impact Assessments ("DPIAs")

12.1 These are a means of assisting the Association in identifying and reducing the risks that our operations have on personal privacy of data subjects.

12.2 The Association shall:

12.2.1 Carry out a DPIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data; and

12.2.2 In carrying out a DPIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data

12.2.3 The Association will require to consult the ICO in the event that a DPIA identifies a high level of risk which cannot be reduced. The Data Protection Officer ("DPO") will be responsible for such reporting, and where a high level of risk is identified by those carrying out the DPIA they require to notify the DPO within five (5) working days.

13. Archiving, Retention and Destruction of Data

The Association cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. The Association shall ensure that all Personal data is archived and destroyed in accordance with the periods specified within the table at Appendix 2 hereto.

Training
All staff will be aware of good practice in data protection and where to find guidance and support for data protection issues.

Adequate and role specific training will be provided regularly to everyone who has access to personal data, to ensure they understand their responsibilities when handling data.

Breach of Policy
Any breaches of this policy, may be considered under the Association's disciplinary procedures, and may result in disciplinary action being taken, including dismissal.

Monitoring and Reporting

Regular audits will be undertaken to check compliance with the law, this policy and any relevant procedures.

List of Appendices

1. Fair Processing Notice
2. Table of Duration of Retention of certain Data
3. Model Data Processor Contract Addendum
4. Model Data Sharing Agreement