Data Protection Policy

1 Introduction

1.1

Background to the General Data Protection Regulation ('GDPR')

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

The Data Protection Act 2018 codifies GDPR into UK Law. For this policy, GDPR 2016 and Data Protection Policy 2018 are used interchangeably to mean the enforceable legislation.

1.2

Scope

The GDPR applies to the processing of personal data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of personal data (i.e. paper records).

1.3

Definitions

Personal Data – any information relating to a person ('data subject'); a person is someone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, mental, economic, cultural or social identity of that person.

Special Categories of Personal Data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Subject – any individual who is the subject of personal data held by PKAVS.

Data Subject Consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child – the GDPR defines a child as anyone under the age of 13 years old. The processing of personal data of a child is only lawful if parental or custodian consent has been obtained. PKAVS shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

2 Policy Statement

2.1 The Board of Directors and management of Perth & Kinross Association of Voluntary Service Ltd. (PKAVS) are committed to compliance with all relevant EU and UK laws in respect of personal data, and the protection of the "rights and freedoms" of individuals whose information PKAVS collects and processes in accordance with the General Data Protection Regulation (GDPR) 2016.

2.2 Compliance with the GDPR is described by this policy and other relevant policies such as PKAVS Information Security Policy and PKAVS Privacy Policy, along with connected processes and procedures.

2.3 The GDPR and this policy apply to all of PKAVS personal data processing functions, including those performed on service users', employees', and volunteers' personal data, and any other personal data PKAVS processes from any source.

2.4 PKAVS' Privacy Officer is responsible for reviewing the register of processing annually in the light of any changes to PKAVS activities (as determined by changes to the data inventory register or PKAVS management review) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the Data Commissioner Office's request.

2.6 This policy applies to all Employees and Volunteers of PKAVS. Any breach of the GDPR will be dealt with under PKAVS Disciplinary Policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.7 Partners and any third parties working with or for PKAVS, and who have or may have access to personal data, will be expected to have read, understood, and to comply with this policy. No third party may access personal data held by PKAVS without having first entered into a data confidentiality agreement (PKAVS Non-disclosure Agreement), which imposes on the third party obligations no less onerous than those to which PKAVS is committed, and which gives PKAVS the right to audit compliance with the agreement.

3 Responsibilities and Roles under the General Data Protection Regulation

3.1 PKAVS is a data controller under the GDPR.

3.2 The Senior Management Team and all those in managerial or supervisory roles throughout PKAVS are responsible for developing and encouraging good information handling practices within PKAVS.

3.3 PKAVS' Privacy Officer is accountable to the Board of Directors of PKAVS for the management of personal data within PKAVS and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

3.3.1 development and implementation of the GDPR as required by this policy; and

3.3.2 security and risk management in relation to compliance with the policy.

3.4 PKAVS' Privacy Officer has been appointed to take responsibility for PKAVS' compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that PKAVS complies with the GDPR, as do Senior Managers in respect of data processing that takes place within their Hub/Service Area.

3.5 PKAVS' Privacy Officer has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for Employees/Volunteers seeking clarification on any aspect of data protection compliance.

3.6 Compliance with data protection legislation is the responsibility of all Employees/Volunteers of PKAVS who process personal data.

3.7 PKAVS GDPR Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees/Volunteers of PKAVS generally.

3.8 Employees/Volunteers of PKAVS are responsible for ensuring that any personal data about them and supplied by them to PKAVS is accurate and up-to-date.

4 Data Protection Principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. PKAVS' policies and procedures are designed to ensure compliance with the principles.

4.1 Personal data must be processed lawfully, fairly, and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent.

Fairly – in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

Transparently – the GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

4.1.1 the contact details of PKAVS Privacy Officer;

4.1.2 the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

4.1.3 the period for which the personal data will be stored;

4.1.4 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

4.1.5 the categories of personal data concerned;

4.1.6 the recipients or categories of recipients of the personal data, where applicable;

4.1.7 any further information necessary to guarantee fair processing.

4.2 Personal data can only be collected for specific, explicit, and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner's Office.

4.3 Personal data must be adequate, relevant, and limited to what is necessary for processing

4.3.1 PKAVS' Privacy Officer is responsible for ensuring that PKAVS does not collect information that is not strictly necessary for the purpose for which it is obtained.

4.3.2 All data collection forms (electronic or paper-based) must include a fair processing statement or link to privacy statement which as been approved by PKAVS' Privacy Officer.

4.3.3 PKAVS Privacy Officer will ensure that, on an annual basis, all data collection methods are reviewed by internal audit to ensure that collected data continues to be adequate, relevant, and not excessive.

4.4 Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

4.4.1 Data that is stored by PKAVS must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.4.2 PKAVS' Privacy Officer is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

4.4.3 Employees/Volunteers are required to notify PKAVS of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of PKAVS to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.4 PKAVS' Privacy Officer is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change, and any other relevant factors.

4.4.5 On at least an annual basis, PKAVS' Privacy Officer will review the retention dates of all the personal data processed by PKAVS, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with PKAVS Information Disposal Procedures.

4.4.6 PKAVS' Privacy Officer is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests. If PKAVS decides not to comply with the request, PKAVS' Privacy Officer must respond to the data subject to explain its reasoning and inform them of their right to complain to the Information Commissioner's Office and seek judicial remedy.

4.5 Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing

4.5.1 Where personal data is retained beyond the processing date, it will be minimised/encrypted/pseudonymised in order to protect the identity of the data subject in the event of a data breach.

4.5.2 Personal data will be retained in line with the PKAVS Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in PKAVS Information Disposal Procedures.

4.5.3 PKAVS' Privacy Officer must specifically approve any data retention that exceeds the retention periods defined in PKAVS Retention of Records Procedure, and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

4.6 Personal data must be processed in a manner that ensures the appropriate security

PKAVS' Privacy Officer, alongside senior managers, will carry out a risk assessment taking into account all the circumstances of PKAVS' controlling or processing operations.

In determining appropriateness, PKAVS' Privacy Officer will also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff, volunteers, or service users) if a security breach occurs, the effect of any security breach on PKAVS itself, and any likely reputational damage including the possible loss of public trust.

When assessing appropriate technical measures, PKAVS' Privacy Officer (alongside PKAVS Information Technology provider/Systems Administrator) will consider the following:

- Password protection;
- Automatic locking of idle electronic computers/devices;
- Removal of access rights for USB and other memory;
- Virus checking software and firewalls;
- Role-based access rights, including those assigned to temporary staff/volunteers;
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local networks;
- Identifying appropriate security standards relevant to PKAVS.

When assessing appropriate organisational measures PKAVS' Privacy Officer will consider the following:

- The appropriate training levels throughout PKAVS;
- Measures that consider the reliability of employees/volunteers (such as references etc.);
- The inclusion of data protection in employment contracts/volunteer agreements;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff/volunteers for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's/volunteer's own personal devices being used in the workplace;

- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

4.7 PKAVS must be able to demonstrate compliance with the GDPR's other principles (accountability)

The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires PKAVS to demonstrate that it complies with the principles and states explicitly that this is its responsibility.

PKAVS will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, data protection impact assessments, breach notification procedures, and incident response plans.

5. Data Subjects' Rights

5.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

5.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

5.1.2 To prevent processing likely to cause damage or distress.

5.1.3 To prevent processing for purposes of direct marketing.

5.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.

5.1.5 To not have significant decisions that will affect them taken solely by automated process.

5.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.

5.1.7 To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.

5.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

5.1.9 To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

5.1.10 To object to any automated profiling that is occurring without consent.

5.2 PKAVS ensures that data subjects may exercise these rights:

5.2.1 Data subjects may make data access requests as described in PKAVS Subject Access Request Procedure; this procedure also describes how PKAVS will ensure that its response to the data access request complies with the requirements of the GDPR.

5.2.2 Data subjects have the right to complain to PKAVS related to the processing of their personal data, the handling of a request from a data subject in line with PKAVS Complaints Procedure.

6 Consent

6.1 PKAVS understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

6.2 PKAVS understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while 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.

6.3 There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication. PKAVS must be able to demonstrate that consent was obtained for the processing operation.

6.4 For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

6.5 In most instances, consent to process personal and sensitive data is obtained routinely by PKAVS using standard consent documents e.g. when a new service user registers, or at employee/volunteer induction.

6.6 Where PKAVS provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16.

7 Security of Data

7.1 All PKAVS' Employees/Volunteers are responsible for ensuring that any personal data that PKAVS holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by PKAVS to receive that information and has entered into a confidentiality agreement.

7.2 All personal data should be accessible only to those who need to use it, and access may only be granted in line with PKAVS Information Security Policy. All personal data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with PKAVS requirements in PKAVS Information Security Policy; and/or
- stored on (removable) computer media which are encrypted in line with the Information Security Policy.

7.3 Care must be taken to ensure that computer screens are not visible except to authorised Employees/Volunteers of PKAVS. All Employees/Volunteers are required to acknowledge PKAVS Information Security Policy before they are given access to organisational information of any sort, which details rules on screen time-outs.

7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day service user support, they must be removed and securely archived or destroyed.

7.5 Personal data may only be deleted or disposed of in line with the Retention of Records Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs/electronic devices are to be removed and immediately destroyed before disposal.

7.6 Processing of personal data 'off-site' presents a potentially greater risk of loss, theft, or damage to personal data. Staff must be specifically authorised to process data off-site.

8. Disclosure of Data

8.1 PKAVS must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Volunteers should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of PKAVS activities.

8.2 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by PKAVS' Privacy Officer.

9. Retention and Disposal of Data

9.1 PKAVS shall not keep personal data in a form that permits identification of data subjects for a longer period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 The retention period for each category of personal data will be set out in the Retention of Records Schedule along with the criteria used to determine this period including any statutory obligations PKAVS has to retain the data.

9.3 PKAVS' data retention and data disposal procedures will apply in all cases.

9.4 Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects. Any disposal of data will be done in accordance with the secure disposal procedure.

10 Information Asset Register/Data Inventory

10.1 PKAVS has established a data inventory as part of its approach to address risks and opportunities throughout its GDPR compliance. PKAVS' data inventory determines:

- organisational processes that use personal data;
- source of personal data;
- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;

- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of PKAVS throughout the data flow;
- key systems and repositories;
- any data transfers; and
- all retention and disposal requirements.

10.2 PKAVS is aware of any risks associated with the processing of particular types of personal data.

10.2.1 PKAVS assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by PKAVS, and in relation to processing undertaken by other organisations on behalf of PKAVS.

10.2.2 PKAVS shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

10.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context, and purposes of the processing is likely to result in a high risk to the rights and freedoms of persons, PKAVS shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

10.2.4 Where, as a result of a DPIA it is clear that PKAVS is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not PKAVS may proceed must be escalated for review to PKAVS' Privacy Officer.

10.2.5 PKAVS' Privacy Officer shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the Information Commissioner's Office.

10.2.6 Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to PKAVS' risk acceptance criteria and the requirements of the GDPR.

Document Owner and Approval

PKAVS' Privacy Officer is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all PKAVS Employees/Volunteers on the PKAVS network and a hard copy will be provided upon request.

This policy was approved by the Board of Directors on 26/04/2018 and is issued on a version controlled basis under the signature of the Chief Executive Officer.

Signature:  Date: 22/05/18

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	PKAVS Board of Directors	22/05/18
2	Updates around Data Protection Act 2018	Information Privacy Officer	31/01/20