Data Protection Policy	KINROSS-SHIRE VOLUNTEER DRIVERS

Context and overview

Introduction

Kinross-shire Volunteer Drivers (KVD) needs to gather and use certain information about individuals.

These include service users, suppliers, business contacts, employees, volunteers and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the charity's data protection requirements – and to comply with the law.

Why this policy exists

This data protection policy ensures KVD:

- Complies with data protection law and follows good practice
- Protects the rights of staff, volunteers, service users and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data Protection Law

The Data Protection Act 2018 describes how organisations, including KVD, must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act 2018 is underpinned by the following principles.

1. Lawfulness, fairness and transparency
2. Purpose limitations
3. Data minimisation
4. Accuracy
5. Storage limitation

6. Integrity and confidentiality
7. Accountability

Lawful Basis

The lawful basis for processing are set out in Article 6 of the General Data Protection Regulation (GDPR). At least one of these must apply whenever KVD process personal data:

(a) Consent: the individual has given clear consent to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract with the individual, or because they have asked to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if a public authority processing data to perform official tasks.)

People, Risks and Responsibilities

Policy Scope

This policy applies to:

- All projects of KVD
- All committee members, staff, and volunteers of KVD
- All contractors, suppliers and other people working on behalf of KVD

It applies to all data that the charity holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 2018. This can include:

- Names of individuals
- Postal Addresses
- Email Addresses
- Telephone numbers
- Plus any other information relating to individuals.

Data protection risks

This policy helps to protect KVD from some very real security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately.
- **Failing to offer choice**. For instance, all individuals should be free to choose how the charity uses data relating to them.
- **Reputational damage.** For instance, the charity could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with KVD has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person that handles personal data must ensure that is handled and processed in line with this policy and data protection principles.

However, the committee members of KVD are responsible for ensuring that KVD meets its legal obligations, by:- .

- Becoming and remaining updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies.
- Arranging any necessary data protection training and advice for people covered by this policy.
- Handling data protection questions from staff, volunteers, service users and anyone else covered by this policy.
- Dealing with requests from individuals to see the data KVD holds about them (also called ‘subject access requests’).
- Checking and approving any contract or agreements with third parties that may handle the charity’s sensitive data.
- Approving any data protection statements attached to communications such as emails
- Address any data protection queries from journalists or media outlets.
- Where necessary, work with other staff to ensure marketing and fundraising initiatives abide by data protection principles.

Staff Guidelines

- The only people able to access data covered by this policy should be those who need it for their work or volunteering with KVD.
- Data should not be shared informally. When access to confidential information is required, employees or volunteers can request it from their line managers and/or the committee of KVD.

- Employees and volunteers should keep all data secure, by taking sensible precautions and following the guidelines below.

    - **Strong passwords must be used** on all files stored and on laptops/computers.

    - Personal data **should not be disclosed** to unauthorised people, either within the charity or externally.

    - Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted if electronically or if paper, shredded.

    - The Employee and volunteers agree to report any actual or suspected data breaches or violations of the Data Protection Policy to their line manager or the committee of KVD immediately.

    - Failure to comply with the Data Protection law regulations may result in disciplinary action, up to and including termination of employment, in accordance with KVD's disciplinary procedures.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the chair of the committee of KVD.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**
- Employees, committee members and volunteers should make sure paper and printouts **are not left where unauthorised people could see them,** for example on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly.
- If data is **stored on removable media** (like DVD, pen drives etc) it should be password protected and these should be kept locked away securely when not being used.

- Data should only be stored on **designated drivers and servers**, if uploaded, only to an approved cloud computing services.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly.
- Data should **never be directly saved to personal laptops** or other **personal** devices such as mobiles devices like tablets or smartphones. (This is different from work machines that back up data onto the charity server).
- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data Use

Personal data is of no value to KVD unless the organisation can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended, and make sure they are **logged out of any database** containing personal information.
- Data must be **password protected before being transferred electronically**.
- Personal data should **not be shared informally**.
- Employees **should not save copies of personal data to their own personal use computers.**

Data Accuracy

The law requires KVD to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees, committee members and volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff, committee members and volunteers should not create unnecessary additional sets of data.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a client's details when they call.
- KVD will make it easy for data subjects to update the information it holds about them.
- Data should be updated as inaccuracies are discovered. For instance, if a volunteer or client can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by KVD are entitled to:

- Ask what information the charity holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the charity is meeting its data protection obligations

If an individual contacts the charity requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by post or email, addressed to the chair of the committee of KVD.

The chair of the committee of KVD. will aim to provide the relevant data within 21 days.

The chair of the committee of KVD will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, the Data Protection Act 2018 allows personal data to be disclosed to law enforcement agencies without consent of the data subject.

Under these circumstances, KVD will disclose requested data. However, the chair of the committee of KVD will ensure the request is legitimate, seeking assistance from committee and legal advisors where necessary.

Providing Information

KVD aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the charity has a Privacy Notice, setting out how data relating to individual is used by the charity.