WESTRIDGE TRUST
DATA PROTECTION POLICY

INTRODUCTION

Westridge Trust needs to gather and use certain information about individuals. These can include customers, suppliers and other people the trust has a relationship with or may need to contact e.g. subscribers to the 100 clubs and individuals supporting fund-raising events. Following the implementation of the General Data Protection Regulation (GDPR) on 24 May 2018 this policy statement has been prepared by the trustees.

WHY THIS POLICY EXISTS

This data protection policy ensures that Westridge Trust:

- Complies with data protection law and follows good practice.
- Protects the rights of customers, staff and other individuals who the trust has a relationship with.
- 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 1998 describes how organisations, including Westridge Trust, 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 is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not to be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not to be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

PEOPLE, RISKS AND RESPONSIBILITIES

POLICY SCOPE

This policy applies to:

- All offices of Westridge Trust
- All staff and volunteers
- All contractors, suppliers and other people working on behalf of Westridge Trust

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers

DATA PROTECTION RISKS

This policy helps to protect Westridge Trust from some very real data security risks, including:

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

RESPONSIBILITIES

Everyone who works for or with Westridge Trust has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles. However, these people have key areas of responsibility:

- The trustees are ultimately responsible for ensuring that Westridge Trust meets its legal obligations.
- The data protection officer, Angela Tiley, is responsible for:
    1. Keeping the board updated about data protection responsibilities, risks and issues.
    2. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    3. Arranging data protection training and advice for the people covered by this policy.
    4. Handling data protection questions from staff and volunteers and anyone else covered by this policy.
    5. Dealing with requests from individuals to see the data Westridge Trust holds about them (also called 'subject access requests').
    6. Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
    7. Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    8. Performing regular checks and scans to ensure security hardware and software is functioning properly.
    9. Evaluating any third-party services the company is considering using to store or process data e.g. cloud computing services.
- The marketing manager, Sally Izett, is responsible for:
    1. Approving any data protection statements attached to communications such as emails and letters.
    2. Addressing any data protection queries from journalists or media outlets.
    3. Where necessary, working with staff and volunteers to ensure marketing initiatives abide by data protection principles.

GENERAL STAFF/VOLUNTEER GUIDELINES

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required this should be requested from the data protection officer.
- Westridge will provide training to all relevant individuals to help them understand their responsibilities when handling data.
- All data should be kept secure by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.

- Data should be reviewed regularly and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the data protection officer.

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 office or filing cabinet.
- Paper and printouts should not be left where unauthorised people could see them e.g. 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, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared.
- If data is stored on removable media such as a DVD or CD, these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- 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, in line with the trust's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
- All computers containing data should be protected by approved security software and a firewall.

DATA USE

Personal data is of no value to Westridge Trust unless the trust 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 computer screens should always be locked when unattended.
- Personal data should not be shared informally. In particular it should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area.

DATA ACCURACY

The law requires Westridge Trust to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort Westridge Trust should put into ensuring its accuracy.

- Data will be held in as few places as necessary.
- Every opportunity should be taken to ensure that data is updated.
- Westridge Trust will make it easy for data subjects to update the information the trust holds about them e.g. via the trust's website.
- Data should be updated as inaccuracies are discovered. For instance, if a supporter 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 Westridge Trust are entitled to:

- Ask what information the trust 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 trust is meeting its data protection obligations.

If an individual contacts the trust requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data protection officer at westridgestudio18@gmail.com who can supply a standard request form, although individuals do not have to use this. The data protection officer will aim to provide the relevant data within 14 days and 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 allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances Westridge Trust will disclose requested data. However, the data protection officer will ensure the request is legitimate, seeking assistance from the board and from the trust's legal advisers where necessary.

PROVIDING INFORMATION

Westridge Trust 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 trust has a privacy notice, which is available on request, setting out how data relating to individuals is used by the trust.