The Westway

The Westway's Policy on Data Protection

Policy Statement

- The Westway collects and uses information about people within the community and with whom it communicates. This personal information must be dealt with properly and securely however it is collected, recorded and used – whether on paper, in a computer or portable electronic device, or recorded on other material – and there are legal safeguards to protect information in the Global Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) (the Acts) and any equivalent subsequent regulation.
- The Westway regards the lawful and correct treatment of personal information as important to the successful and efficient performance of its functions and to maintain confidence between those with whom it deals.
- To this end The Westway endorses and adheres to the Principles of Data Protection, as set out in the Acts and subsequent legislation.
- This Policy should be read in conjunction with (1) The Westway web-based Privacy Policy and (2) The Westway's Policy on Business Continuity Management, which specifically refers to data storage and IT security.

Purpose

- The purpose of this policy is to ensure that the staff, volunteers and Trustees of The Westway are clear about the purpose and principles of Data Protection and to ensure that The Westway has guidelines and procedures in place which are consistently followed.
- Failure to adhere to the Acts and subsequent legislation is unlawful and could result in legal action being taken against The Westway or its staff, volunteers or Trustees.
- Everyone who works for or with The Westway has some responsibility for ensuring data is collected, stored and handled appropriately.

Principles

- The Acts regulate the processing of information relating to living and identifiable individuals (data subjects). This includes the obtaining, holding, using or disclosing of such information and covers electronic records as well as manual filing systems, including card indexes.

- Data users must comply with the data protection principles of good practice which underpin the Act. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.
- To do this The Westway follows the eight Data Protection Principles outlined in the Acts, which are summarised below:
  I. Personal data will be processed fairly and lawfully
  II. Data will only be collected and used for specified purposes
  III. Data will be adequate, relevant and not excessive
  IV. Data will be accurate and up to date
  V. Data will not be held any longer than necessary
  VI. Data subject's rights will be respected
  VII. Data will be kept safe from unauthorised access, accidental loss or damage
  VIII. Data will not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

The Principles apply to "personal data" which is information held on electronic or in manual filing systems from which they are identifiable. The Westway's employees, volunteers and Trustees who process or use any personal information in the course of their duties will ensure that these principles are followed at all times.

The Risks

This policy is aimed to protect The Westway from actual data security risk, including:

- Breaches of confidentiality – information being given out inappropriately;
- Failing to offer choice – individuals should be free to choose how a corporate uses data relating to them, and
- Reputational damage - if an unauthorised third-party gained access to sensitive data.

Procedures

- The following procedures have been developed in order to ensure that The Westway meets its responsibilities in terms of Data Protection. For the purposes of these procedures data collected, stored and used by The Westway falls into two broad categories:
  1. The Westway's internal data records - staff, volunteers and Trustees
  2. The Westway's external data records - members, customers, clients.
- The Westway as a body is a DATA CONTROLLER under the Act, and the Board of Trustees is ultimately responsible for the policy's implementation.

General staff guidelines

- The Westway operates a "Clear Desk Policy" at all times.
- 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, employees can request it from their line manager.
- The Westway will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure by taking sensible precautions and following the guidelines contained in this policy.

- Strong passwords must be used and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within The Westway 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 and disposed of in accordance with the schedule detailed below.
- Employees should request help and advice from the General Manager if they are unsure about any aspect of data protection.
- The contact details of staff, volunteers and Trustees will only made available to other staff, volunteers and Trustees. Any other information supplied on application will be kept in a secure filing cabinet or data-file and is not accessed during the day-to-day running of the charity.
- Contact details of staff, volunteers and Trustees will not be passed on to anyone outside the organisation without their explicit consent.
- A copy of staff, volunteer, Trustee emergency contact details will be kept in the Business Continuity Management Policy dossier and by the General Manager.
- Upon request, staff, volunteers and Trustees will be supplied with a copy of their personal data held by the charity.
- All confidential post must be opened by the addressee only.

Data storage

These rules describe how and where data should be safely stored.

- When data is stored on paper, it should be kept in a secure place where unauthorised personnel 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 locked filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer or photo-copier.
- 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 between employees.
- If data is stored on removable media (like a thumb-drive), these should be encrypted and kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded. Storage in the “Cloud” is not permitted with the exception of the “QuickBooks” application.
- 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 company’s standard back-up procedures.
- Personal data should never be saved directly to mobile devices like smart phones.
- 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 The Westway unless the charity has a specific use for 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 and volunteers should ensure the screens of their computers are always locked when left 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. The General Manager can explain how to send data to authorised external contacts.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

Data accuracy

- The law requires The Westway 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 The Westway should put into ensuring its accuracy.
- It is the responsibility of all employees 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 should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- The staff of The Westway will make it easy for data subjects to update the information it holds about them. For instance, via the website.
- Data should be updated as and when inaccuracies are discovered. For instance, if a volunteer can no longer be reached on their stored telephone number, it should be removed from the database.
- The Westway will take reasonable steps to keep personal data up to date and accurate. Personal data will be stored for 20 years after an employee, volunteer or Trustee has worked for the organisation and brief details for longer. Unless the organisation is specifically asked by an individual to destroy their details it will normally keep them on file for future reference. The General Manager has responsibility for destroying personnel files.

Subject access requests

All individuals who are the subject of personal data held by The Westway 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 company is meeting its data protection obligations.

If an individual contacts The Westway requesting this information, this is called a *Subject Access Request*. Subject access requests from individuals should be made by email, addressed to the General Manager at info@tva.org.uk. The General Manager can supply a standard request form, although individuals do not have to use this. Individuals will be charged £10 per subject access request. The General Manager will aim to provide the

relevant data within 14 days, who will, of course, verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

- In certain circumstances, the Acts allow personal data to be disclosed to law enforcement agencies without the consent of the data subject.
- Under these circumstances, The Westway will disclose requested data. However, the General Manager will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

The Westway 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 Westway has a web-based privacy statement, setting out how data relating to individuals is used by the charity.
- Internal data records.

Purposes

The Westway obtains personal data (names, addresses, telephone numbers, email addresses), application forms, and references and in some cases other documents from staff, volunteers and Trustees. This data is stored and processed for the following purposes:

- Recruitment;
- Equal Opportunities monitoring;
- The objectives of The Westway including volunteering opportunities;
- To distribute relevant organisational material, e.g. meeting papers;
- Payroll.

Storage

- Personal data is kept in paper-based systems and on a password-protected computer system. Every effort is made to ensure that data is stored in organised and secure systems.
- The Westway always operates a clear desk policy .

Use of Photographs

Where practicable, The Westway will seek consent from individuals before displaying photographs in which they appear. If this is not possible (for example, a large group photo), the organisation will remove any photograph if a complaint is received. This policy also applies to photographs published on The Westway's website or in our publications.

Use of the Cloud and International Access

- The Board of Trustees has agreed not to use Cloud-Computing for storage. The exception to this rule is the use of the finance application "QuickBooks", which is used as the accounting package for The Westway and contains no personal information.
- In accordance with the Acts no electronic data relevant to The Westway should be stored internationally.

External data records

Purposes

- The Westway obtains personal data (such as names, addresses, and telephone numbers) from members/clients. This data is obtained, stored and processed solely to assist staff and volunteers in the efficient running of services. Personal details supplied are only used to send material that is potentially useful. Most of this information is stored on the organisation's database.
- The Westway obtains personal data and information from clients and members in order to provide services. This data is stored and processed only for the purposes outlined in the agreement and service specification signed by the client/member.

Consent

- Personal data is collected over the telephone by correspondence and using other methods such as e-mail. During this initial contact, the data owner is given an explanation of how this information will be used, in accordance with the Acts.
- Personal data will not be passed on to anyone outside the organisation without explicit consent from the data owner unless there is a legal duty of disclosure under other legislation, in which case the General Manager will discuss and agree disclosure with the Chair/Vice Chair. Only if consent has been given will contact details held on The Westway's database be made available to groups/individuals outside of the organisation. Individuals must be made aware of when their details are being collected for the database and their written consent given.

Access

- Only The Westway's staff, volunteers and Trustees will normally have access to personal data. All staff, volunteers and Trustees are made aware of the Data Protection Policy and their obligation not to disclose personal data to anyone who is not supposed to have it.
- Information supplied is kept in a secure filing, paper and electronic system and is only accessed by those individuals involved in the delivery of the service.
- Information will not be passed on to anyone outside of The Westway without their explicit consent, except under legal requirement, e.g. the Inland Revenue.
- Individuals will be supplied with a copy of any of their personal data held by The Westway if a request is made.
- All confidential post must be opened by the addressee only.

Accuracy

- The Westway will take reasonable steps to keep personal data up to date and accurate. Personal data will be stored for as long as the data owner/client/member uses our services and normally longer. Where an individual ceases to use our services and it is not deemed appropriate to keep their records, their records will be destroyed. Records will be destroyed in accordance with the Acts requirements.
- If a request is received from an organisation/individual to destroy their records, The Westway will remove their details from the database and request that all staff holding paper or electronic details for the organisation destroy them.

Storage

- Personal data may be kept in paper-based systems and on a password-protected computer system. Paper-based data are stored in organised and secure systems.
- The Westway operates a clear desk policy at all times.

Use of Photographs

- Where practicable, The Westway will seek consent of members/individuals before displaying photographs in which they appear. If this is not possible (for example, a large

group photo), The Westway will remove any photograph if a complaint is received. This policy also applies to photographs published on The Westway's website or publications.

Disclosure and Barring Service

- The Westway will act in accordance with the Disclosure and Barring Service's (DBS) code of practice.
- Copies of disclosures are kept for no longer than is required. In most cases this is no longer than six months in accordance with the DBS Code of Practice. There may be circumstance where it is deemed appropriate to exceed this limit e.g. in the case of disputes.

Responsibilities of staff, volunteers and Trustees

- During the course of their duties with The Westway, staff, volunteers and Trustees will be dealing with information such as names/addresses/telephone numbers/e-mail addresses of members/clients/volunteers. They may be told or overhear sensitive information while working for The Westway. The Acts and subsequent legislation give specific guidance on how this information should be dealt with. In short, to comply with the law, personal information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. Staff, paid or unpaid must abide by this policy.

Compliance

- Compliance with the Act is the responsibility of all staff, paid or unpaid. The Westway will regard any unlawful breach of any provision of the Act by any staff, paid or unpaid, as a serious matter which will result in disciplinary action. Any employee who breaches this policy statement will be dealt with under the disciplinary procedure which may result in dismissal for gross misconduct. Any such breach could also lead to criminal prosecution.
- Any questions or concerns about the interpretation or operation of this policy statement should in the first instance be referred to the General Manager.

Retention of Data (see schedule below)

- No documents or personal data will be stored for longer than is appropriate.
- All documents containing personal data will be disposed of securely in accordance with the Data Protection principles.

Approved by: Chair of Trustees, The Westway

Date of Approval:

Date of Review:

DOCUMENT	RETENTION		Reference to Archive means scanned and electronically filed
Type	Description	Retention period	Disposal action
Governance			
Board and sub-committee agendas, supporting papers and minutes	Provides an audit trail of statutory compliance, a corporate memory of decisions and is of historical value to the organisation	Permanent	Archive
Corporate business plans and annual reports	Provides an audit trail of statutory compliance, a corporate memory of decisions and is of historical value to the organisation	Permanent	Archive
General			
Registration	Details of corporate registrations and organisational links	Current year plus 6	Archive
General Enquiries	If record taken	6 months	Destroy
Procedure			
Procedure Manuals	Process documentation	When superseded	Destroy
Policy Documents	Part of supporting governance	Permanent	Archive
Disclosure and Barring Service		6 Months	Archive
Human Resources			
Recruitment, appointment and/or promotion papers		1 year	Archive
Personnel Files (Job History)	Written particulars of employment, Contracts of employment, changes to terms and conditions, including change of hours letters	Current year plus 20	Archive
Qualifications and references		Current year plus 6	Destroy
Staff address details		6 years after employment has ended	Destroy
Pay History	Personal payroll history, including record of pay, performance pay, overtime pay, allowances, pay enhancements, other taxable allowances, payment for untaken leave, reduced pay, no pay, maternity leave	Current year plus 20	Archive
Annual Leave records		2 years	Destroy
Other Leave Records		Current year plus 20	Destroy
Training History		6 years	Destroy
Performance Reviews and/or Assessments	Reports or summary of Performance papers for last five years of service	15 Years after Service	Destroy
Notice of end of employment letter	Resignation, termination and/or Retirement letters	15 years after service	Destroy
Leaver files		15 years after service	Destroy
Health			
Health Declarations		Current year plus 20	Archive
Sickness Absence records		Current year plus 20	Archive
Records relating to workplace injury		Current plus 20 years	Archive
Finance			
Summaries of daily banking and statements	Daily reports of transactions	Current year plus 2	Destroy
Petty cash records	Records/books/sheets and receipts	Current year plus 2	Destroy
Staff expenses	Reimbursement forms for travel etc.	Current year plus 6	Destroy
Invoices	Invoices/debit notices rendered on debtors (invoices paid, unpaid, registers of invoices, debtors ledgers etc)	Current year plus 6	Destroy

Refunds	Records relating to unrecoverable revenue, debts and overpayments	Current year plus 6	Destroy
VAT	Receipt Books/Records for Imposts (Stamp Duty/VAT)	Current year plus 6	Destroy
Employee Pay history		Current year plus 6	Destroy
Salaries/wages payroll		Current year plus 2	Destroy
Employee pay history		Current year plus 6	Destroy
Salary/Wages payroll sheets		Current year plus 2	Destroy
Budgets & formal interim reports		Current year plus 6	Destroy
Financial Statements	Statements prepared for inclusion in quarterly or annual reports	Current year plus 6	Destroy
Budget working papers	Draft papers or material for creating yearly or quarterly budgets	Current year plus 3	Destroy
Final Budget Reports		Current year plus 10	Destroy
Other financial documents		Current year plus 3	Destroy
Financial working papers		Current year plus 2	
Theft			
Theft/Fraud (resolved internally)	Relating to serious matters of theft, fraud, misappropriation, irrecoverable debts and overpayments, write-offs, recovery of debt, wavering of debt where the matter was resolved internally	6 years after closure	Archive
Theft/Fraud (resolved Externally)	Relating to serious matters of theft, fraud, misappropriation, irrecoverable debts and overpayments, write-offs, recovery of debt, wavering of debt where external action was taken	10 years from closure	Archive
Audit Reports Internal		Current year plus 3	Archive
Working papers and reports		Current year plus 3	
Annual Audit report external	(These include interim reports) where audit has included the examination of long-term contracts	Current year plus 6	

Approved by: Chair of Trustees, The Westway

Date of Approval: 21 April 2018

Date of Review: April 2019