Westgate Foundation: Policies Handbook

Policy No: 106/18

Policy Name: Data Protection Policy

Westgate Foundation, West Village, Ballincollig, Co. Cork	**Approval date** 21/05/2018	**Revision Date** 22/05/2019
Responsibility for approval of policy	Governance Sub-Group	
Responsibility for implementation	CEO : Julie Murphy and Managers Team	
Responsibility for ensuring review	CEO: Julie Murphy	

Policy Statement

Westgate Foundation is committed to the protection and welfare of our clients, staff, members, residents, students, work placement personnel, volunteers, suppliers and contractors. As part of this commitment Westgate Foundation will do all within its powers to ensure that all data relating to all of the above is secured and retained in compliance with Data Protection Legislation. (Data Protection Act 2018).

Purpose

The purpose of this policy is to detail the principles, protocols and procedures that will be followed within the organisation to safeguard all data secured and held by the organisation.

Scope

Compliance with this policy applies to Westgate Foundation employees, volunteers, service users, placement students, members and anyone acting under the auspices of Westgate Foundation.

Officer responsible within the organisation: Julie Murphy, CEO Westgate Foundation (Data Controller for the organisation). All managers within Westgate Foundation are expected to facilitate and support the implementation of this policy.

Policy No: 106/18

Policy Name: Data Protection Policy

Introduction:

Westgate Foundation needs to gather and use certain information about individuals. These can include clients, members, residents, service users, staff, volunteers, work placements and student placements, suppliers, contractors 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 company's data protection standards and to comply with the law.

Why this policy exists:

This Data Protection Policy ensures that Westgate Foundation:

- Complies with data protection law and follows good practice
- Protects the rights of staff, clients, members, residents, volunteers, student and work placements, contractor, suppliers and any other people the organisation engages 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 Westgate Foundation- must collect, handle and store personal information.

These rules apply regardless of whether the 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 8 important principles. These say that personal data must:

Policy No: 106/18

Policy Name: Data Protection Policy

- Be processed fairly and lawfully
- Be obtained only for specific lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held longer than is necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not 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 services of Westgate Foundation
- All staff, volunteers and work/student placement personnel
- All contractors, suppliers and other people working on behalf of Westgate Foundation.

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
- Any other information relating to individuals

Data Protection Risks:

Policy No: 106/18

Policy Name: Data Protection Policy

This policy helps to protect Westgate Foundation from some very real data 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 company uses date relating to them
- Reputational Damage: For instance the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities:

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

General Staff 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 employees can request it from their line managers
- **Westgate Foundation 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 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 **regularly reviewed and updated** if it is found to be out of date. If no longer required it should be securely deleted and disposed of, as appropriate to regulations regarding data storage.
- Employees **should request help** from their line manager or the Data Controller (DPO) if they are unsure of any aspect of data protection.

Data Storage:

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

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 should make sure paper and printouts are **not left where unauthorised people could see them, like 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 login passwords** that will be regularly and never shared between employees
- If data is **stored on removable media** (like a CD, USB or DVD) 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 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, in line with the company's standard backup procedures
- **Personal** data should **never be saved directly to laptop**s or other mobile devices like tablets or 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 Westgate Foundation, unless the business 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
- 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 password protected before being transferred electronically.** The IT 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.

Policy No: 106/18

Policy Name: Data Protection Policy

Data Accuracy:

The law requires Westgate Foundation 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 Westgate Foundation 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**. Client, member, resident, staff, volunteer, student placement, supplier and contractor databases will be reviewed annually to ensure all details are accurate.
- Westgate Foundation will make it **possible for data subjects to request updates to the information** Westgate Foundation holds about them.
- Data should **be updated as inaccuracies are discovered**. For instance, if a client can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requirements:

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

- Ask **what information** the company 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 company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email or post, addressed to the data controller at Westgate Foundation. The data controller can supply a standard request form although the individuals do not have to use this.

The data controller will always verify the identity of anyone making a subject access request before handing over 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, Westgate Foundation will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and form the company's legal advisors where necessary.

Providing Information

Westgate Foundation 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 company has a privacy statement, setting out how data relating to individuals is used by the company. This is available on request. A version of this statement is also available on the company's website.

Policy No: 106/18

Policy Name: Data Protection Policy

Key Day to Day Protocols and Procedures:

- Personal Data can only be accessed with Line Manager approval
- All line managers must be clear on their purposes for accessing personal data
- Personal Data must be kept in secure - (locked- paper files or password protected – soft files).
- All line managers must know where the personal data relevant to their department is stored
- Personal date should only be shared with other managers on a need to know basis only.
- All personal data will be reviewed annually and updated.
- General communication regarding Westgate Foundation's data management policies, procedures and protocols will be issued through the Data Controller (CEO).
- Personal Data should never be uploaded or downloaded on to mobile devices (USB Keys, Laptops, CDs/DVDs, Mobile Phone data files).

Policy No: 106/18

Policy Name: Data Protection Policy

Policy No: 106/18

Policy Name: Data Protection Policy