westgate

Data protection

3 April 2018

Policy prepared by:	Westgate Communications Ltd
Approved by the Directors on:	3rd April 2018
Next review date:	31st March 2019
Data Protection Registration Number (ico.):	Z2184271

Introduction

Westgate Communications Ltd needs to gather and use certain information about individuals.

This can include customers, suppliers, business contacts, employees and other people that the organisation has a relationship with or which it 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 Westgate Communications Ltd:

- Complies with data protection law and follows good practice.
- Protects the rights of staff, customers and partners.
- Is open about how it stores and processes each individual's data.
- Protects itself from the risks of a data breach.

Data protection law

The Data Protection Act 1998 describes how organisations, including Westgate Communications Ltd, 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.

Westgate Communications Ltd ensure that personal information is:

1. processed fairly and lawfully.
2. obtained only for specified, lawful purposes.
3. adequate, relevant and not excessive.
4. 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. 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 staff of Westgate Communications Ltd.
- All contractors, suppliers and other people working on behalf of Westgate Communications Ltd.

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.
- …plus any other information relating to individuals.

Data protection risks
This policy helps to protect Westgate Communications Ltd 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 data relating to them.

Reputational damage.
For instance, the company could suffer if hackers successfully gained access to sensitive data.

People, risks and responsibilities

continued

Responsibilities
Everyone who works for or with Westgate Communications Ltd has some responsibility for ensuring that 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 **directors** are ultimately responsible for ensuring that Westgate Communications Ltd meets its legal obligations.

The Westgate Communications Ltd Data Management Team is responsible for:

- Keeping directors and all staff updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data Westgate Communications Ltd hold about them (also called subject access requests).
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from other staff to ensure marketing initiatives abide by data protection principles.

People, risks and responsibilities

continued

Responsibilities *continued*
The Westgate Communications Ltd IT Manager is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

General 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 Communications Ltd 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 deleted and disposed of.
- Employees **should request help** from their line manager or the **Data Management Team** if they are unsure about 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 Data Management Team, 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 when unauthorised people could see them, such as 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 and never shared between employees.
  - If personal data is stored on removable media (like a CD or DVD), these should only be uploaded to approved Westgate secure personal data storage areas on Google.
  - Servers containing personal data should be sited in a secure location, away from general office space.
  - Personal data backups need to be made in an appropriate and secure manner.
  - All personal data stored on laptop or mobile devices should only be stored on an approved Westgate Google account address book – personal data should never be saved to any other area of a laptop or mobile device.
  - All data transfers outside the network should be encrypted.
  - 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 Communications Ltd 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 if not secure.

- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised external contacts.

- 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 Westgate Communications Ltd 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 Communications Ltd 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.

Westgate Communications Ltd will make it easy for individuals to update the information Westgate Communications Ltd hold about them. For instance, via the Westgate Communications Ltd Google Drive.

- Data **should be updated as inaccuracies are discovered**. For instance, if a customer 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 Westgate Communications Ltd 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**.

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

Subject access requests from individuals should ideally be made by email, addressed to the data controller at Westgate Communications Ltd, 58 Cobden Road, Sevenoaks, Kent TN13 3UB. The data controller can supply a standard request form, although individuals do not have to use this.

The data controller will aim to provide the relevant data within 40 days.

The data controller 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, Westgate Communications Ltd will disclose requested data. However, Westgate Communications Ltd will ensure the request is legitimate, seeking assistance from the board and from the our legal advisers where necessary.

Providing information

Westgate Communications Ltd 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.

westgate

Further details

If you require clarity or further information, please contact us on:

Telephone 01732 779 087
info@westgatecomms.com

Westgate Communications Ltd
Registered number 4414399
VAT Number 830555147

www.westgatecomms.com