# Data Protection Policy

Context and overview

## Key Details:

- Policy prepared by Selective Group
- Operational on: 25th May 2018
- Review Date: 25th May 2019

## Introduction

Selective Group needs to gather and use certain information about individuals. These individuals include: Residential tenants (prospective and current), business tenants (prospective and current), Livery customers, guarantors, business contacts, employees and other people the company 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.

This policy will be implemented in conjunction with the following other policies:

- Retention Policy
- Fair Processing Notice
- CCTV Policy (for College Farm Site)
- Information Asset Register

## Why this policy exists

This data protection policy ensures that Selective Group:

- 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 individuals' data
- Protects itself from the risks of a data breach

## Data Protection Law

This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'

The above legislation describes how organisations – including Selective Group – 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 regulations are underpinned by the following important principle:

Personal data must:

- 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 any longer than necessary
- Processed in accordance with the rights of the data subjects
- Be protected in appropriate ways
- 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 and contractors working for Selective Group

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

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Any other information relating to individuals

### Data protection risks

This policy helps to protect Selective Group from some very real data security risks including:

- Breaches of confidentiality – for example, information being given out inappropriately
- Failing to offer choice – for example, all individuals should be free to chooses how the company uses data relating to them
- Reputational damage – for example, the company could suffer if hackers successfully gained access to sensitive data

### Responsibilities

Everyone who works for, or on behalf of, has some responsibility for ensuring that data is collected, stored and handled correctly. All who handle 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:

- Wendy and Chris Whistler as partners of Selective Group are ultimately responsible for
    - Ensuring that Selective Group meets its legal obligations
    - Ensure they are aware of data protection responsibilities, risks and issues
    - Annually reviewing all data protection procedures and policies
    - Handling Data protection questions from staff and anyone else covered by this policy
    - Dealing with requests from individuals to see the data Selective Group holds about them (also known as Subject Access Requests – SAR)

- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data
- Ensuring all systems, services and equipment used for storing data meets acceptable security standards
- Preforming 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 Staff guidelines

- The only people able to access data covered by this policy should be those who need it for work
- Data should not be shared informally.
- Selective Group 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 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 if they're unsure about any aspect of data protection

### Data Storage

The rules describe how and whether data should be safely stored. Questions bot storing data can be directed to Chris and Wendy Whistler

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 that paper and printouts are not left where unauthorised people could see them, like 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 (like data stick or cd) these should be kept locked away securely when not in use
- Data should only be store don 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 and these backups tested regularly
- Data should never be saved directly to laptops or other mobile devices like tablets or smartphones
- 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 Selective Group 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 cannot be overlooked and 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 unless password protected
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area (EEA)
- 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 Selective Group to take reasonable steps to ensure that data is kept accurate and up to date. The more important it is that personal data is accurate, the greater the effort Selective Group should put into ensuring its accuracy. It is the responsibility of all employees who work with data to take reasonable steps to ensure that it is kept as accurate and up to date as possible.

- Data will be kept in a few places as necessary. Staff should not create any unnecessary additional data sets
- Staff should take every opportunity to ensure that data is updated. For example, by confirming a customer's details when they call
- Selective Group will make it easy for data subjects to update the information Selective Group holds about them
- Data should be updated as inaccuracies are discovered. For example, if a customer can no longer reached on their stored telephone number, it should be removed from the data base.

## Subject Access Requests

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

- Ask what information is held by the company 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 to request this information, it is called a Subject Access Request (SAR)

SARs from individuals should be made by email, addressed to the Data Protection Officer (Wendy Whistler) at wendy@selectivegroup.co.uk. Information will be provided, where possible, within 14 days

The Data Protection Officer will always verify the identity of anyone making a SAR request before handing over any information.

### Disclosing data for other reasons

In certain circumstances, The GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject

Under these circumstances, Selective Group will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance where necessary.

### Providing Information

Selective Group 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 fair processing notice setting out how data relating to individuals is used by the company. This is available on our website or upon request to info@selectivegroup.co.uk