Fleet Components

Data Protection Policy – January 2018

Introduction

Fleet Components needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people that we have a relationship with or may need to contact.
This Policy describes how this personal data must be collected, handled and stored to meet our data protection standards — and to comply with the law.

Why Policy Exists

This Data Protection Policy ensures that the Company:

- 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

Personal Data Definition

Personal Data, which falls within these guidelines, is defined as any information (both current and historic) that could be used on its own or in conjunction with any other data to identify an individual person. This includes anything from a name, photo, email address, bank details, CCTV footage, posts on social networking websites, medical information, phone numbers, addresses, or a computer I.P. address.

As well as information concerning employees and members of the public, the scope of the new legislation will also include volunteers and fundraisers.

Data Protection Law

The new Data Protection Regime Regulations (GDPR) are effective from May 2018, these describe how organisations — including ours must collect, handle and store personal information.
These rules apply regardless of whether data is stored electronically, on paper or on other materials and includes photographs of individuals, CCTV footage and social media posts.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.
The regulations are underpinned by a number of 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 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 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 of our premises/offices from which we operate
- All of our staff and any volunteers or fundraisers
  All customers and members of the public of which we may come into contact with and hold data on
- All contractors, suppliers and other people working on behalf of ourselves.

In summary, it applies to all data that the Company holds relating to identifiable individuals, even if that information technically falls outside of previous Data Legislation including the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
  Internet I.P. addresses
  CCTV footage and photographs of individuals
  Posts on social media sites
- Any other information relating to individuals that can be used to identify them

Data Protection Obligations

Specifically, explicit consent must be obtained from individuals to use, store and manage their personal data. This has to be done whilst disclosing the intended use and duration of the storage of the data. It also needs to be demonstrated that the opportunity of withdrawing consent must be made as easy as giving consent.

Data Protection Risks

This Policy helps to protect our organisation 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.

Responsibilities

Everyone who works for or with our Company has some responsibility for ensuring data is collected, stored, protected and handled appropriately.
Each person 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:

- Simon Gamlin is ultimately responsible for ensuring that we meet our legal obligations.
- Simon Gamlin is responsible for:
    - Keeping the Company updated about data protection responsibilities, risks and issues.
      Appointing a Data Protection Controller for our organisation – our Data Protection Controller is Ross Parker
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging any necessary data protection training and advice for the people covered by this Policy.
      Ensuring explicit consent is obtained from individuals to use, store and manage their personal data.
    - Handling data protection questions from staff and anyone else covered by this Policy.
    - Dealing with requests from individuals to see what data we hold about them (also called ‘subject access requests’).
      Dealing with requests to remove personal data.
      Ensuring that personal data is removed if the data is no longer being used for the purposes that it was collected
    - 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 journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Ensuring regular checks and scans are carried out 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

- This policy is applicable to all staff – see specifically the previously identified definitions of 'Personal Data' – including CCTV footage, photographs, posts on social media sites etc. Staff should therefore only access personal data if it is needed for their work.
- Data should not be shared informally. This includes not giving out anything that can be used to identify a subject/individual. When access to confidential information is required, employees can request it from their Manager.
- We will provide training to all employees as necessary 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 Manager 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 Director Simon Gamlin Or Ross Parker
When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access 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 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 between employees.
- If data is stored on removable media (like a CD, DVD or USB), 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 Company 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.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones. In particular, data should not be saved or stored on personal devices.
- All servers and computers containing data should be protected by approved security software and a firewall as appropriate.

Data Use

Personal data is of no commercial value to our organisation 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 encrypted before being transferred electronically. The Data Controller 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 or personal devices. Always access and update the central copy of any data.

Data Accuracy

The law requires us to take reasonable steps to ensure data is kept accurate and up to date.
It is important that the personal data is accurate, and we therefore need to take great effort 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 Company will make it easy for data subjects to update the information that we hold about them. This could include for example, via the Company website.
- Data should be updated as soon 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 the Company are entitled to:

- Ask what information we hold about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how we are meeting our data protection obligations.
  Request and be granted the removal of personal data either if they no longer want us to hold it or if it is no longer being used for the purpose it was collected.

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, addressed to the Managing Director /Data Controller at ross@devonfleet.co.uk or simon@devonfleet.co.uk 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 14 days of the request.
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 legislation allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, the Company will disclose requested data. However, the Data Controller will ensure the request is legitimate, seeking assistance from the Managing Director and from the Company's Legal Advisers where necessary.

Providing Information

The Company 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 privacy statement is available on request.