Data Protection Policy

Fleet Development Ltd & Associated Organisations

Data Protection Policy

Policy information	
Organisation	Gary Clark is responsible as the Data Controller. "Data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed "Data processor", in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Fleet Development Ltd is the organisation responsible for the management of this policy Classic Bus Hire T/A Fleet Development is a Fleet Development Ltd organisation Classic Bus Hire Ltd is a Fleet Development organisation The Organisation is any Fleet Development organisation
Scope of policy	This policy applies to all Fleet Development organisations.
Policy operational date	See below.
Policy prepared by	Gary Clark
Date approved by Board/ Management Committee	May 2018
Policy review date	At least yearly or as required in the event of legislative changes.

Introduction	
Purpose of policy	• Complying with the law • Following good practice • Protecting clients, staff and other individuals • Protecting the organisation
Types of data	This policy aims to protect all types of client and staff data.
Policy statement	Fleet Development gives a commitment to: • Comply with both the law and good practice • Respect individuals' rights • Be open and honest with individuals whose data is held • Provide training and support for staff who handle personal data, so that they can act confidently and consistently Please note the guidance from ICO on when breaches should be reported as this is one of the main changes from the current Data Protection Act and GDPR Please also note the information on individuals' rights. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/
Key risks	Key risks to Fleet Development are identified as: • Information about data getting into the wrong hands, through poor security or inappropriate disclosure of information • Individuals being harmed through data being inaccurate or insufficient

Responsibilities

The Board / Company Directors	They have overall responsibility for ensuring that the organisation complies with its legal obligations.
Data Protection Officer	Gary Clark is the Data Protection Officer. Their responsibilities include: • Briefing the Board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Employees & Volunteers	All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'employees' is used, this includes both paid employees and volunteers.)
Enforcement	We will offer training where appropriate to those colleagues reporting difficulty adjusting to the requirements of this procedure. Continued breaches (more than one per 12 month period) by colleagues may result in action being taken in accordance with the Fleet Development Disciplinary Procedure

Security	
Scope	Data Security is not wholly a Data Protection issue.
Setting security levels	The greater the consequences of a breach of confidentiality, the tighter the security should be. To address security we may take disciplinary action against colleagues breaching this policy
Security measures	Fleet Development shall ensure confidential data is stored with password being required to access the files. We will never intentionally pass your details to any third party unless we have your prior written permission.
Business continuity	Fleet Development have a Business Continuity Plan. This is stored in a secure location and only available to senior members of staff
Specific risks	Special precautions to be taken when information is in particularly risky situations, such as being worked on at home, with clients, at meetings, etc. Potential to provide details over the phone or during social /public gatherings.

Data recording and storage	
Accuracy	Fleet Development will strive to ensure 100% accuracy when recording information. We will check details with you at the time and may confirm after the event. We will record where the data originated but shall endeavour not to share your data without your prior written permission. In this case we shall ensure we record who we share your data with.
Updating	We may periodically update the information we hold about you. If we have a continuing relationship with you we will hold onto the data for no more than 24months after our last interaction at which point we will securely archive your data. If we have a single transaction with you we will securely archive your data no later than six months after our interaction.
Storage	We store data securely on our IT system or in locked storage files
Retention periods	See Updating. We may also for legal reasons hold onto your data even after you have withdrawn your consent for us to hold your data. See Lawful Basis below.
Archiving	We will securely store any archived data in a password protected IT location. Access will be limited to senior company management and will require two signatures prior to release. We reserve the right to use cloud based systems for the archiving of data. In such case we will ensure we follow all applicable guideline. We will not publish the method of retention used unless specifically requested and unless relevant. Paper copies of document shall be shredded on our premises with copies held electronically.

Right of Access

Responsibility	Gary Clark is responsible for Rights of Access requests.
Procedure for making request	Right of access requests must be in writing. We will accept requests by post or email but NOT in any way verbally. Requests should be clear detailing what Is required. We will respond within the one month of request but do reserve the right to extend this time frame, but we will inform you as soon as possible of this development. An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone).
Provision for verifying identity	If we are unable to verify your identity we may request information to assist us in arriving at the correct result. If we are unable to verify your identity we will refuse any request for information you present.
Charging	We will attempt to provide the information free of charge. We may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. We may charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests. The fee will be based on the administrative cost of providing the information.

Transparency	
Commitment	We are committed to transparency and shall ensure we cooperate fully with any requests made.
Procedure	We shall provide the following methods to ensure our colleagues and clients are informed about this policy • The handbook for employees • In the welcome letter or pack for members, with occasional reminders in the newsletter • On the web site
Responsibility	Gary Clark is responsible for all aspects of transparency.

Lawful Basis	
Underlying principles	What are the lawful bases for processing? The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data: **(a) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose. **(b) Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. **(c) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations). **(d) Vital interests:** the processing is necessary to protect someone's life. **(e) Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. **(f) Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)
Opting out	Fleet Development does not currently use any facility where consent requests such as opting in via a tick box are used.
Withdrawing consent	Fleet Development acknowledge that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where the organisation has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn

Employee training & Acceptance of responsibilities	
Induction	All employees who have access to any kind of personal data should have their responsibilities outlined during their induction procedures
Continuing training	If there are opportunities to raise Data Protection issues during employee training, team meetings, supervisions, etc.
Procedure for staff signifying acceptance of policy	All Fleet Development Staff (including non directly employed Staff) will be required to sign to demonstrate acceptance of this policy.

Policy review	
Responsibility	Gary Clark is responsible for this policy
Procedure	The Senior Management team shall agree any changes to the policy
Timing	This policy shall be reviewed at least every 12 months or earlier in case of legislative changes

For more information, please visit the ICO website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/