**Data Protection Policy**

**Context & Overview**

**Key details**

* Policy prepared by: **Christopher Wootton**
* Approved by board / management on: 11/11/2019
* Policy became operational on: 11/11/2019
* Next review date: 10/11/2020

**Introduction**

**Formula Escapes Ltd** needs to gather and use certain information about individuals.
These can include customers, suppliers, business contacts, employees 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. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.
The Company is committed not only to the letter of the law but also to the spirit of the law and places a high premium on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.
The Company is registered with the Information Commissioner as a data controller under the register held by the Information Commissioner pursuant to Section 19 of the Act.

**Why this policy exists**

This data protection policy ensures **Formula Escapes Ltd:**

* Complies with data protection law and follow 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**

The Data Protection Act 1998 describes how organisations — including **Formula Escapes 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.
The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
This Policy sets the Company’s obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.
The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.
The Data Protection Act is underpinned by eight 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

**The Rights of Data Subjects**

The GDPR sets out the following rights applicable to data subjects for which this Data Protection Policy addresses:

* The right to be informed;
* The right of access;
* The right to rectification;
* The right to erasure (also known as the ‘right to be forgotten’);
* The right to restrict processing;
* The right to data portability;
* The right to object; and
* Rights with respect to automated decision-making and profiling

**Lawful, Fair, and Transparent Data Processing**

1. The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:
	1. The data subject has given consent to the processing of their personal data for one or more specific purposes;
	2. The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
	3. The processing is necessary for compliance with a legal obligation to which the data controller is subject;
	4. The processing is necessary to protect the vital interests of the data subject or of another natural person;
	5. The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
	6. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
2. If the personal data in question is “special category data” (also known as “sensitive personal data”) (for example, data concerning the data subject’s race, ethnicity, health, sex life, or sexual orientation), at least one of the following conditions must be met:
	* 1. The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
		2. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
		3. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
		4. The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
		5. The processing relates to personal data which is clearly made public by the data subject;
		6. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
		7. The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
		8. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
		9. The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
		10. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

**People, risks and responsibilities**

**Policy scope**

This policy applies to:

* The head office of **Formula Escapes Ltd**
* All branches of**Formula Escapes Ltd**
* All staff and volunteers of**Formula Escapes Ltd**
* All contractors, suppliers and other people working on behalf of **Formula Escapes 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
* Data required for provision of services – e.g. Passport Details

**Personal Data Collected, Held, and Processed**
Personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company’s Data Retention Policy):
Please refer to our Data Audits for details of how this data is managed.

**Data protection risks**

This policy helps to protect **Formula Escapes Ltd** from 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 **Formula Escapes Ltd** has some responsibility for ensuring 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 board of directors are ultimately responsible for ensuring that**Formula Escapes Ltd** meets its legal obligations.
* The **data protection officer, Christopher Wootton**is responsible for:
	+ Keeping the board 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 [company name] holds 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.
* The **IT manager, Christopher Wootton**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.
* The **marketing manager, Christopher Wootton** is responsible for:
	+ 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.

**General staff guidelines**

1. The only people able to access data covered by this policy should be those who need it for their work.
2. Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
3. **Formula Escapes Ltd** will provide training to all employees to help them understand their responsibilities when handling data.
4. Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
5. In particular, strong passwords must be used and they should never be shared.
6. Personal data should not be disclosed to unauthorised people, either within the company or externally.
7. 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.
8. Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

**Keeping Data Subjects Informed**

1. The Company shall provide the information set out in Part 12. to every data subject:
2. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
3. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
	1. if the personal data is used to communicate with the data subject, when the first communication is made; or
	2. if the personal data is to be transferred to another party, before that transfer is made; or
	3. as soon as reasonably possible and in any event not more than one month after the personal data is obtained.
4. The following information shall be provided:
	1. Details of the Company including, but not limited to, the identity of its Data Protection Contact / Officer;
	2. The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing;
	3. Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data;
	4. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
	5. Where the personal data is to be transferred to one or more third parties, details of those parties;
	6. Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the “EEA”), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);
	7. Details of data retention;
	8. Details of the data subject’s rights under the GDPR;
	9. Details of the data subject’s right to withdraw their consent to the Company’s processing of their personal data at any time;
	10. Details of the data subject’s right to complain to the Information Commissioner’s Office (the “supervisory authority” under the GDPR);
	11. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
	12. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any

**Objections to Personal Data Processing**

1. Data subjects have the right to object to the Company processing their personal data based on legitimate interests, direct marketing (including profiling),
2. Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company’s legitimate grounds for such processing override the data subject’s interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
3. Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing immediately.

**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 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 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.
* Data should **never be saved directly**to laptops or other mobile devices like tablets or smart phones.
* No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).
* 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 **Formula Escapes 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 is not secure.
* Data must be **encrypted 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.

**Data accuracy**

The law requires **Formula Escapes 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**Formula Escapes Ltd** will 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.
* **Formula Escapes Ltd**  will make it **easy for data subjects to update the information Formula Escapes Ltd** holds about them. Data subjects can update their information by emailing**chris@formulaescapes.com**
* 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.
* It is the marketing manager’s responsibility to ensure**marketing databases are checked against industry suppression files**every six months.

**Data Retention**

* The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
* When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
* For full details of the Company’s approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Privacy Policy

**Subject access requests**

All individuals who are the subject of personal data held by **Formula Escapes 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.**
* 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, addressed to the data controller at **chris@formulaescapes.com**. The data controller can supply a standard request form, although individuals do not have to use this.
Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 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, **Formula Escapes Ltd** will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company’s legal advisers where necessary.
**Transferring Personal Data to a Country Outside the EEA**

1. The Company may from time to time transfer (‘transfer’ includes making available remotely) personal data to countries outside of the EEA.
2. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
	1. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
	2. The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner’s Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
	3. The transfer is made with the informed consent of the relevant data subject(s);
	4. The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject);
	5. The transfer is necessary for important public interest reasons;
	6. The transfer is necessary for the conduct of legal claims;
	7. The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
	8. The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

**Providing information**

**Formula Escapes 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.