# VENTURE FORCE: DATA PROTECTION POLICY
# MAY 2019

**Policy Statement**

Venture Force is committed to safeguarding and protecting the privacy of all stakeholders.

Venture Force collects and uses information about people with whom it communicates and for whom it organises and manages Expeditions. This personal information must be dealt with properly and securely however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the GDPR 2018.

Venture Force regards the lawful and correct treatment of personal information as fundamental to the successful and efficient performance of its functions, and to maintain confidence between those with whom it works. To this end Venture Force fully endorses and adheres to the Principles of Data Protection, as set out in the GDPR 2018.

**Purpose**

The purpose of this policy is:

- to ensure that the staff, contractors and volunteers of Venture Force are clear about the purpose and principles of Data Protection and to ensure that Venture Force has guidelines and procedures in place that are consistently followed.
- To demonstrate to our partners and those Organisations that we work with that we have systems in place to safeguard any of their personal data that we collect and, for appropriate reasons, share with other interested parties.

Failure to properly protect Data is unlawful and could result in legal action being taken against Venture Force, its staff, its contracts, or its volunteers.

**Principles**

The GDPR regulates the processing of information relating to living and identifiable individuals (data subjects). This includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems.

**Data users must comply with the data protection principles of good practice that underpin the Regulations.** To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

To do this Venture Force follows the Principles outlined in Article 5 of GDPR, which are summarised below:

- Personal data will be processed fairly and lawfully
- Data will **only** be collected and used for **specified purposes**
- Data will be **adequate, relevant and not excessive**
- Data will be **accurate** and **up to date**
- Data will not be held any longer than necessary

- Data subject's rights will be respected
- Data will be kept safe from unauthorised access, accidental loss or damage.
- Data will not routinely be transferred to a country outside of the UK unless and until any recipient has contracted to uphold the requirements of GDPR and to safeguard any such data according to these requirements
- It may sometimes be necessary to transfer personal information overseas. Any transfers made will be in compliance with the GDPR. In some instances Venture Force will need to provide personal data to local agents outside the European Economic area in order to apply for named permits or in order to provide emergency support. Venture Force enter in to contracts with local agents appropriately to protect the personal data of all its stakeholders.

The principles apply to "personal data" which is information held on computer or in manual filing systems from which data subjects are identifiable. Venture Force employees and volunteers who process or use any personal information in the course of their duties will ensure that these principles are followed at all times.

GDPR regards Personal Data as meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier and can include some or all of the following: name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Sensitive Personal Information including but not limited to information on physical & mental health, ethnicity, sexual orientation, financial details, require more careful handling and will only be collected with consent and when it is absolutely essential in the conduct of our work.

**Data Handling**

The General Data Protection Regulation regulates data processing relating to living and identifiable individuals. This includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems. The principles apply to "personal and sensitive personal data" from which the subjects of that data are identifiable. Venture Force's staff, volunteers, contractors and partners who process, use or have access to any personal information in the course of their duties will ensure that these principles are followed at all times.

**Undertaking to Data Owners**

Venture Force undertakes to:

- seek your consent to hold your personal and sensitive data.
- only hold your personal data for as long as is necessary for clearly specified purposes
- be clear with you why we collect personal and sensitive data, why we need it, and who will have access to it
- only share personal and sensitive information with relevant persons to enable them to undertake specific duties for Venture Force
- seek your consent to hold your personal data should you join the Venture Force Community
- not share your personal data with third parties for their marketing purposes.
- take appropriate measures to ensure that your personal information is protected from unauthorised access or modification, unlawful destruction and improper use.
- allow you to see records of any correspondence, personal and or sensitive data you have sent to us
- respond positively to any query or complaint about our data handling policy

- make every effort to secure consent from staff, clients, contractors and volunteers before displaying images in which they appear. Our contractual arrangements with clients include in-perpetuity permission to publish all images, on any platform, in connection with their expeditions with Venture Force. We will however remove any image from the public domain, if it is within our power to do so, if a complaint is received or if consent is not given.

* It may sometimes be necessary to transfer personal information overseas. Any transfers made will be in compliance with the GDPR. In some instances Venture Force will need to provide personal data to local agents outside the European Economic area in order to apply for named permits or in order to provide emergency support. Venture Force enter in to contracts with local agents appropriately to protect the personal data of all its stakeholders.

**How do we collect personal and sensitive personal information?**

Personal information and/or sensitive personal information is collected in a variety of ways, including but not limited to:

- Client applications
- Staff employment applications
- Leader Applications
- Expedition journals / video or written diaries
- Recruitment information such as interviews and interview notes
- Sponsored events registrations
- Fundraising forms
- Requests for information
- Feedback forms
- Venture Force Community commitments

Venture Force may also collect personal information and/or sensitive personal information when you download / upload resources from our website, complete a survey or if you contact us by email. We also use software to identify which areas of our site are visited most frequently. This helps us to understand how our website is being used so that we can make it more useful for visitors.

**What is personal and sensitive personal information collected used for?**

The information we collect may be used to:

- process applications, establish identity
- process payments
- keep a record of essential contact details
- Enact any operational procedures including evacuations support evaluation
- Engage staff
- Pay staff
- Maintain personnel records
- Engage leaders and teachers and make any appropriate arrangements for them
- Respond to requests for information
- Business purposes including changing and improving levels of service

**Who is information shared with?**

We sometimes need to share the personal and sensitive information we process with the data subject (s), and with other organisations. Where this is necessary we are required to comply with all aspects of the GDPR. This means that any Data to be shared will be:

- Processed fairly, lawfully and in a transparent manner
- Processed for limited, defined purposes and in an appropriate way
- Adequate, relevant and not excessive for the purpose
- Accurate and up to date
- Not kept longer than necessary for the purpose
- Processed in line with data subject's rights
- Secure
- Not transferred to people or organisations without adequate protection

The following is a list of the types of organisations with whom we may need to share some of the personal or sensitive information we process for one or more reasons. Where strictly necessary we share information with:

- Family, associates or representatives of the person whose personal data we are processing (i.e. designated next of kin or emergency contact details)
- Other Expedition Members and / or their parents
- Employees
- Leaders & teachers
- Partners
- Contractors
- Third party service providers including emergency services
- Current employers
- Healthcare, social and welfare organisations
- Statutory bodies including HMRC
- Providers of goods and services
- Educator and examining bodies
- Financial organisations
- Business associates and professional advisers
- Police Forces

**Procedures**

The following procedures have been developed in order to ensure that Venture Force meets its responsibilities in terms of Data Protection. For the purposes of these procedures data collected, stored and used by Venture Force falls into 3 categories:

1. Venture Force's internal data records – Staff, Contractors and Volunteers

2. Venture Force's external data records – Customers, clients and teachers

3. Venture Force's external data records – Subcontractors and In-Country Staff

Venture Force as a body is a **DATA CONTROLLER**, and the Directors are ultimately responsible for the policy's implementation. See Appendix 1 for Definitions.

## INTERNAL DATA RECORDS

### Purposes

Venture Force obtains personal data (names, addresses, phone numbers, Next of Kin details, email addresses) application forms, references and in some cases other documents from staff, contractors and volunteers. This data is stored and processed for the following purposes:

- Recruitment
- To distribute relevant organisational material
- Payroll
- Access
- To meet statutory obligations (Charity Commission, Companies House, etc) Record System and used only for the purposes for which it was given or in the event of an emergency.
- To meet Health and Safety requirements

The contact details of staff, contractors & volunteers will only be made available as appropriate to other staff, contractors and volunteers. All information supplied on application will be kept in soft copy and used only for the purpose for which it was supplied. Contact details of staff, contractors and volunteers will not be passed on to anyone outside* the organisation without their explicit consent. All staff, contractor and volunteer emergency contact details will be securely electronically stored in our Record System and used only for the purposes for which it was given or in the event of an emergency.

**DBS / PVG -** Venture Force requires all staff, contractors and volunteers to supply enhanced DBS / PVG checks. We will act in accordance with the DBS's code of practice. Copies of disclosures, when they are supplied, are kept for no longer than is required. DBS Certificates will only be shared with relevant staff in the course of recruitment and vetting duties. Teachers accompanying expeditions with their own school pupil will not be required to supply Venture Force with a DBS certificate. This is covered by their contract with their employer.

### Accuracy & Access

Staff, contractors and volunteers may be supplied with a copy of their personal data held by us if a written request is made to one of the Directors. All post that is marked confidential will be forwarded to be opened by the addressee only. Venture Force operates a password-protected computer system and all desktop and laptop machines are encrypted.

## EXTERNAL DATA RECORDS

### Purposes

Venture Force obtains personal data (such as names, addresses, and phone numbers) from customers /clients and from their Next of Kin. We also collect sensitive data such as medical information from our clients. This data is obtained, stored and processed to assist staff in the efficient running of services and to ensure high standards of care and positive experiences for our venturers, leaders and all expedition participants. This personal and sensitive data is stored and processed only for the purposes outlined in the contract signed by clients or as otherwise authorised (for example by acknowledging terms and conditions online) by the client.

### Consent

As part of the application process applicants are required to acknowledge our Terms and Conditions and our Data and Privacy Protection Policy. Personal and sensitive data may also be updated/collected over the phone and using other methods such as e-mail. This will only occur *after* clients have already consented to the collection of personal and sensitive data and will remain within the same scope of collection, processing and use as already consented to.

### Clients

Venture Force works with young adults; we are aware of the necessity to be sensitive to the needs of young and/or vulnerable data owners/subjects. Applicants under the age of 18 are required to secure adult consent for their participation in an Expedition. We use clear language and transparency in all our communication with clients, particularly those under the age of 18, to ensure that they understand what we mean by sensitive and personal data.

### Access

Only key staff will normally be given access to personal and sensitive data. All staff, contractors and volunteers are made aware of our Data Protection Policy and of their obligation to handle personal data with absolute discretion. Information supplied is kept in secure paper and electronic systems and is only accessed by those individuals involved in the delivery of the service. By necessity when leaders take information with them on expedition leaders are advised to store the data as safety and securely as possibly. Information will not be passed on to anyone outside the organisation without explicit consent. Some forms of such consent are included in our contractual arrangements with our clients in case of emergencies. Individuals who make a formal request to see any data held by us will be supplied with a copy of any of their personal and sensitive data held by Venture Force within 10 days.

### Accuracy

Venture Force will take regular steps to keep personal data up to date and accurate by contacting data subjects/owners. Personal and sensitive data will be stored only for the duration of the planning of an expedition and only for as long as necessary thereafter. All data will be destroyed in a manner that complies with the guidelines. If an error in our personal and sensitive data is identified by an individual and we receive a request from them to amend their records during our retention period, we will do so if we can verify the identity of the individual and can confirm the accuracy of the amend.

**Sharing of data**

Our work requires us from time to time to share specific pieces of personal and sensitive information with key staff members, contractors, volunteers, teachers and partner organisations. Some of these organisations are based outside the European Economic Area and wherever possible this information remains digital, is password protected, and is retained within Venture Force's electronic file system. Whilst on expedition, we may need to provide paper documentation to a limited number of individuals and/or organisations for whom digital access cannot be assured. In any such cases we will record 'who and where' so as to assure the location of and subsequent safe destruction of any and all data shared in this way. In some circumstances, outside of the European Economic Area, Venture Force may be required for the performance of a contract to provide data in order to access a service (for example a National Park) without a guarantee of a chain of custody or Data Privacy Policy. In these circumstances Venture Force can accept no liability for the safety of personal or sensitive data.

**Storage**

Personal data will be kept on a password-protected and encrypted computer system that is backed up securely.

**RETENTION OF DATA**

No documents will be stored for longer than is necessary after the return of an Expedition.

Leaders, contractors, volunteers and teacher's data will be retained until such time as we receive a request from the data subject to delete the data.

Staff data will be retained for 6 months after employment ceases.

Recruitment documentation relating to unsuccessful applicants will be deleted after 12 months from the final interview date unless we receive a request from an unsuccessful applicant to retain their information in relation to potential future opportunities. Recruitment documentation relating to successfully appointed staff will be retained until 6 months after their employment ceases or 1 year from the interview date, which ever is the greater.

All documents containing personal and sensitive data will be disposed of securely in accordance with Data Protection principles.

# Annex 1

## Definitions

**Data Controller** – legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

**Data Processor** – 'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

**Personal Information** - information that identifies someone as an individual and may include some or all of the following:

- Personal details
- Family details
- Lifestyle & social circumstance
- financial
- education & employment
- visual images

**Sensitive personal information** is information about an individual's

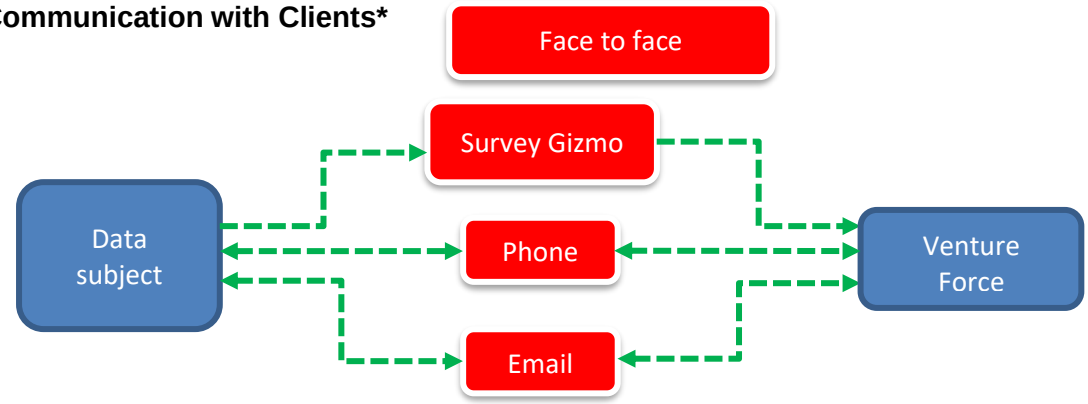
- physical or mental health details
- racial or ethnic origin
- religious or other beliefs of a similar nature
- offences and alleged offences
- criminal proceedings, outcomes and sentences

**Key staff** - are defined as the Directors, permeant employees, expedition managers, operations room staff, medical advisor and in-country agents.

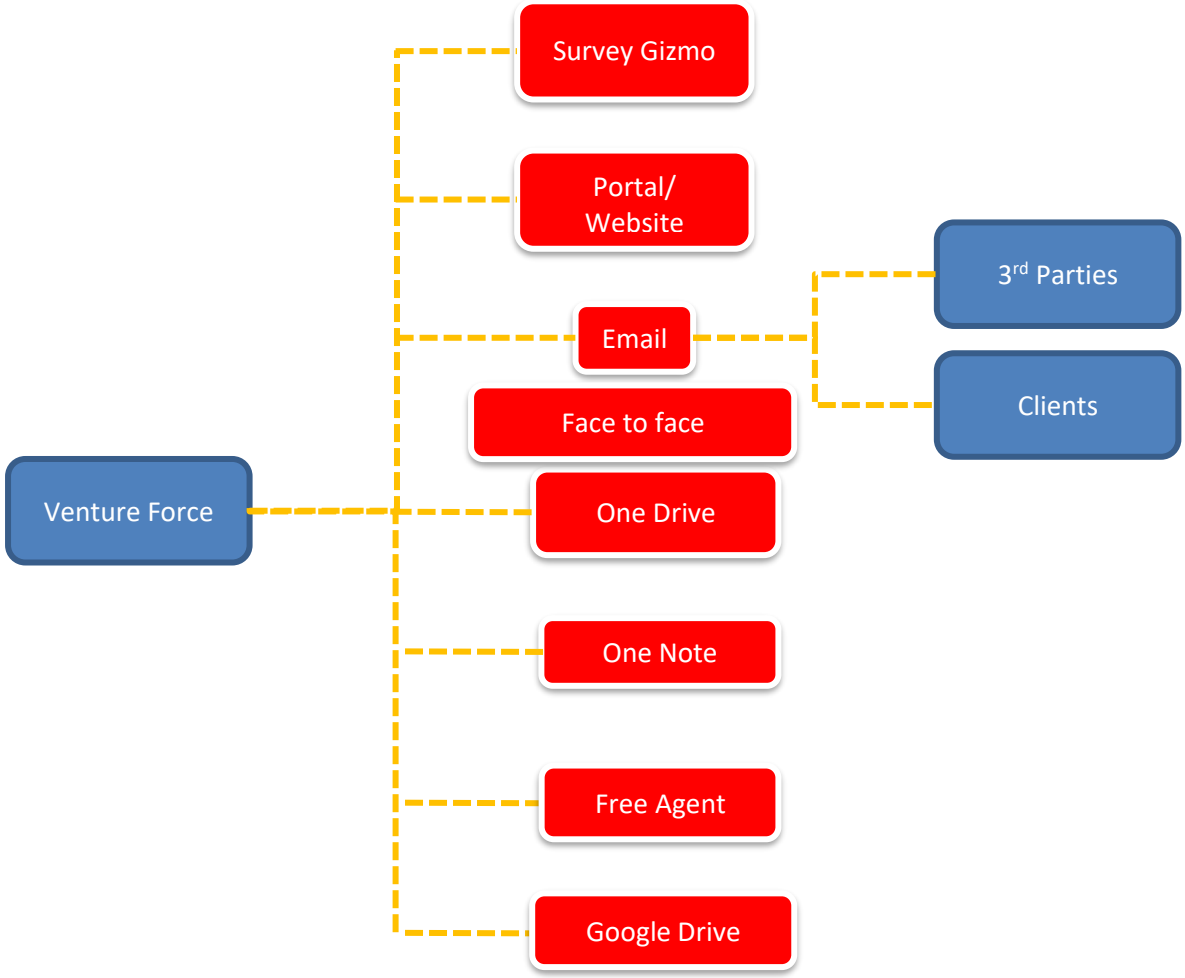
**Client** – means client or in the case of a client who is under 18 that person plus any adult with parental responsibilities.

# Annex 2

**Communication with Clients***




**Data Processing and Storage***




**Further details relating to how data is collected, processed and stored are provided in the sections below.*

**What platforms do we use to store data and how are they protected?**

- Survey Gizmo – SSL Certificate in place – https:// makes data uploaded and transit from clients secure
- Portal/Website – SSL certificate in place
- Emails – Secure Exchange Accounts
- Microsoft Office 365 Business Package
- Free Agent - Encrypted
- Laptops – Encrypted

**Types of data**

Personal Information

- Personal details
- Family details
- Lifestyle/social circumstances
- Financial details
- Education + employment
- Images

Sensitive Information

- Physical or mental health details
- Religious beliefs
- Offences
- Criminal proceedings

**How do we collect data?**

- School sign-up forms/ tear-off slips
- Online data collection/medical forms
- Consent Forms and Contracts
- Document Uploads – website e.g. passport copies
- Leader Applications
- Leader Information Update Forms
- Staff recruitment
- Newsletter subscriptions
- Job applications
- Email requests
- Phone requests
- Feedback forms
- Fundraising registrations
- Invoices

**What do we use this data for?**

- Process Applications
- Establish Identity
- Keep a record of key contact details
- Keep a record of emergency contacts
- Process Client Payments
- Pay staff + contractors
- Enable expedition managers to book flights, accommodation + transport

- Enable office staff to safely manage the expedition
- Enable expedition managers to arrange travel permits + visas
- To enable pre-departure medical screening
- To enable Venture Force leaders to run a safe expedition
- To enable the VF Operations Room to manage in-country incidents including supporting evacuations
- Promote and Market Venture Force and its' products
- Respond to requests for information
- Provide newsletters or event details: contact stakeholders about current + future work carried our by Venture Force
- Maintain personnel records
- For business purposes including data analysis, audits, fraud prevention, modifying/improving services. Identifying sign-up trends, expending our operational reach
- As we believe to be necessary or appropriate under the law in compliance with legal processes and to respond to requests from government authorities
- To allow us to respond to complaints or incidents
- To limit damages which could be sustained to venture Force

**Who do we share data with and what do we share?**

- Family, associates or representatives of the person whose personal data we are processing (e.g. designated NOK or emergency contacts) – data relevant to the safe management of the expedition
- Venture Force key staff – Full details to allow for the safe management of the expedition throughout
- Venture Force Volunteers – Name, gender, date of birth, passport details, medical details, dietary requirements and any other data required for the safe management of the expedition
- School Teachers involved in the development and delivery of the expedition – Name, gender, date of birth, passport details, medical details, dietary requirements and any other data required for the safe management of the expedition
- Flights Agent/Airline – Name, date of birth, gender, passport details, dietary requirements
- Accommodations – Name, date of birth, gender and passport details as required for the purpose of booking and staying at accommodation in country
- Other parents – We will share participant names for the purpose of issuing the expedition confirmation note, ATOL certificate and for visa documentation
- Fogg Insurance – Name and expedition destination
- Remote Medical Services – Name, date of birth and medical information
- Venture Force Operations Room – Full details to allow for the safe management of the expedition
- School Emergency Contact – Full details to allow for the safe management of the expedition
- Medical Advisor - Name, date of birth and medical information
- Statutory bodies including HMRC or police forces
- Business associates and professional advisers
- Survey organisations
- 3rd parties service providers e.g. National Parks/Permit Organisations – Name, date of birth, gender + passport details

**How long do we keep data for?**

- In the case of clients, parents, NOK/Emergency Contact + Teachers, we will keep the data for no longer than necessary following the end of the expeditions return

- Where an incident occurs, relevant data will be kept for 3 years or until the incident/complaint has been fully resolved.
- For leaders and contractors, we will keep data until such time as we receive a request from the data subject to delete the data.
- For 3rd parties including school teachers, we will keep data until such time as we receive a request from the data subject to delete the data.
- For employees, data will be kept for 6 months following the end of their contract.

**How do we delete data?**

Data will be disposed of securely, as per GDPR requirements, once the retention period has expired or following a request for data to be deleted.

Anybody can request for a copy of their data at any point and request that data stored on them is deleted with immediate effect. Any such request for deletion of data may only be granted if all other requirements are met.