VENTURE FORCE: DATA PROTECTION POLICY

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 into 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 and mental health, ethnicity, sexual orientation, financial details, requires 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 promptly and positively to any query or complaint about our data handling practices
- 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.

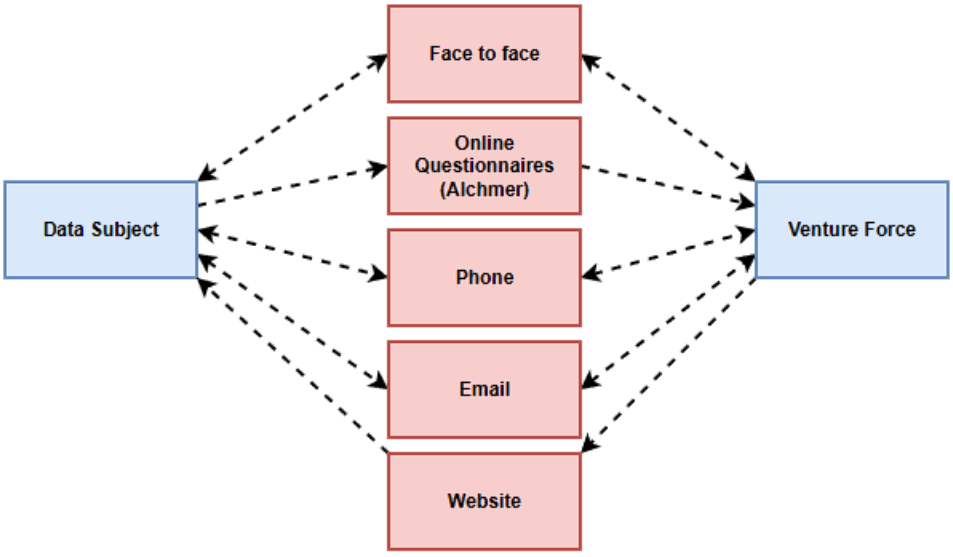
USE OF MESSAGING SERVICES

Venture Force may use encrypted messaging services such as WhatsApp to support expedition delivery. This includes creating group chats for adult expedition teams or leaders/customer staff to facilitate introductions and logistics prior to departure, using leader-to-doctor communication groups for non-emergency medical queries, and sharing relevant documents with in-country agents. These groups are managed securely, and participants are instructed not to share sensitive personal data within chat threads. Documents shared via WhatsApp are reviewed for necessity, appropriateness, and, where possible, are password protected.

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 expedition applications and related forms
- Staff employment applications
- Leader applications
- Recruitment processes, including interviews and interview notes
- Sponsored event registrations
- Fundraising forms
- Feedback forms
- Requests for information
- Venture Force community commitments
- Website interactions, such as uploading or downloading resources, completing surveys, or submitting contact forms



We may also collect certain data automatically when users visit our website. This includes information about which pages are visited most frequently. This helps us analyse how the site is used and improve the user experience.

The information we collect may be used to:

- Process applications and confirm identity
- Process payments and maintain financial records
- Keep a record of essential contact details
- Respond to requests for information
- Engage and pay staff, leaders, and contractors
- Maintain personnel and HR records
- Make arrangements for staff and expedition leaders, including travel, accommodation, insurance, and emergency contact details
- Enact operational procedures related to expeditions, including logistics, safety, risk management, medical arrangements, and emergency planning
- Share relevant personal data with third parties involved in the expedition (e.g. airlines, insurance providers, in-country partners) where necessary for the delivery of the expedition
- Maintain contact before, during and after the expedition for operational and safeguarding purposes
- Communicate important updates or changes to the expedition
- Use anonymised or summarised data for internal business purposes, including monitoring, evaluation, and service improvement

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 or individuals with whom we may need to share personal or sensitive information, where it is strictly necessary and lawful to do so for operational, legal, or safeguarding reasons:

- **Next of kin or emergency contacts** – family members, associates, or representatives of the individual
- **Other expedition participants and/or their parents or guardians** – where necessary for coordination or safeguarding
- **Expedition staff** – including employed staff, contracted leaders, and customer-provided staff (e.g. teachers, group leaders)
- **In-country partners and contractors** – including accommodation providers, transport companies, and ground agents
- **Third-party service providers** – such as airlines, insurance companies, emergency assistance providers, or logistics support

- **Healthcare providers and welfare organisations** – where necessary for medical treatment or safeguarding
- **Statutory authorities** – including HMRC, immigration authorities, border control, and the police
- **Education providers and examining bodies** – where relevant to expedition-related qualifications or reporting
- **Financial institutions** – for processing payments or refunds
- **Professional advisers and business associates** – such as legal, HR, IT, or safeguarding consultants
- **Customers** – where the expedition is organised through a school or other client organisation
- **Suppliers of goods and services** – for delivery of equipment, clothing, or other expedition-related needs

PROCEDURES

The following procedures have been developed in order to ensure that Venture Force meets its responsibilities in terms of Data Protection. All aspects of the procedures are carried out in compliance with Venture Force's Information Security Policy.

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 (e.g. Charity Commission, Companies House), and to ensure emergency preparedness. This information is stored in our secure Record System and used only for the purpose for which it was provided 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. School staff/customer staff accompanying expeditions with young people from their own organisation are not required to supply a DBS certificate to Venture Force, as this responsibility remains with their employer under existing safeguarding arrangements.

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. Where expedition leaders are required to take data with them, they are advised to store this information as safely and securely as possible, and to ensure it is disposed of responsibly once no longer required. 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 such circumstances, where data is shared beyond the European Economic Area without assurance of a data privacy policy or custodial chain, Venture Force cannot guarantee the continued protection of the data in line with UK standards.

STORAGE

Personal data will be kept on a password-protected and encrypted computer system that is backed up securely. All aspects of storage will be carried out in compliance with Venture Force's Information Security Policy.

RETENTION OF DATA

Venture Force retains personal and sensitive data only for as long as necessary for the purpose for which it was collected and in line with our operational, legal, and safeguarding obligations.

- **Participant names and email addresses** are retained after an expedition for marketing purposes. An opt-out link is provided in the final expedition communication, and all marketing emails include a clear unsubscribe option.
- **Expedition documentation** (including medical and consent forms) is retained for **1 year** after the expedition concludes, after which it is securely deleted.
- **Contract documentation** is retained for **6 years** in line with legal and financial regulations.
- **Finance documentation** (such as payment records and invoices) is also retained for **6 years**.
- **Complaints or incident reports** are retained for **3 years** from the date of resolution.
- **Leaders, contractors, and volunteers' data** will be retained until a request is received from the individual for its deletion or until we no longer have a legitimate business need to hold it.
- **Staff data** will be retained for **6 months** after employment ends.

- **Recruitment documentation** for unsuccessful applicants is retained for **12 months** from the final interview date, unless the applicant requests that their details be retained for future opportunities.
- **Recruitment documentation** for successful applicants is retained until **6 months after employment ends** or **1 year from the interview date**, whichever is later.

All documents containing personal or sensitive data are disposed of securely in accordance with data protection principles.

For more information on how long we retain specific categories of data, please refer to our **Data Retention Calendar**.

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. All deletion processes are carried out in accordance with Venture Force's Information Security Policy, which outlines secure disposal procedures for both physical and digital records.

Individuals have the right to request a copy of their personal data at any time. Venture Force will respond to such requests within the timeframe required by law and may need to verify the identity of the requester before releasing any data. Requests for deletion of personal data will also be honoured, provided that the data is no longer required for legal, operational, or safeguarding purposes.

DATA PROCESSING AND STORAGE

WHAT PLATFORMS DO WE USE TO STORE DATA AND HOW ARE THEY PROTECTED?

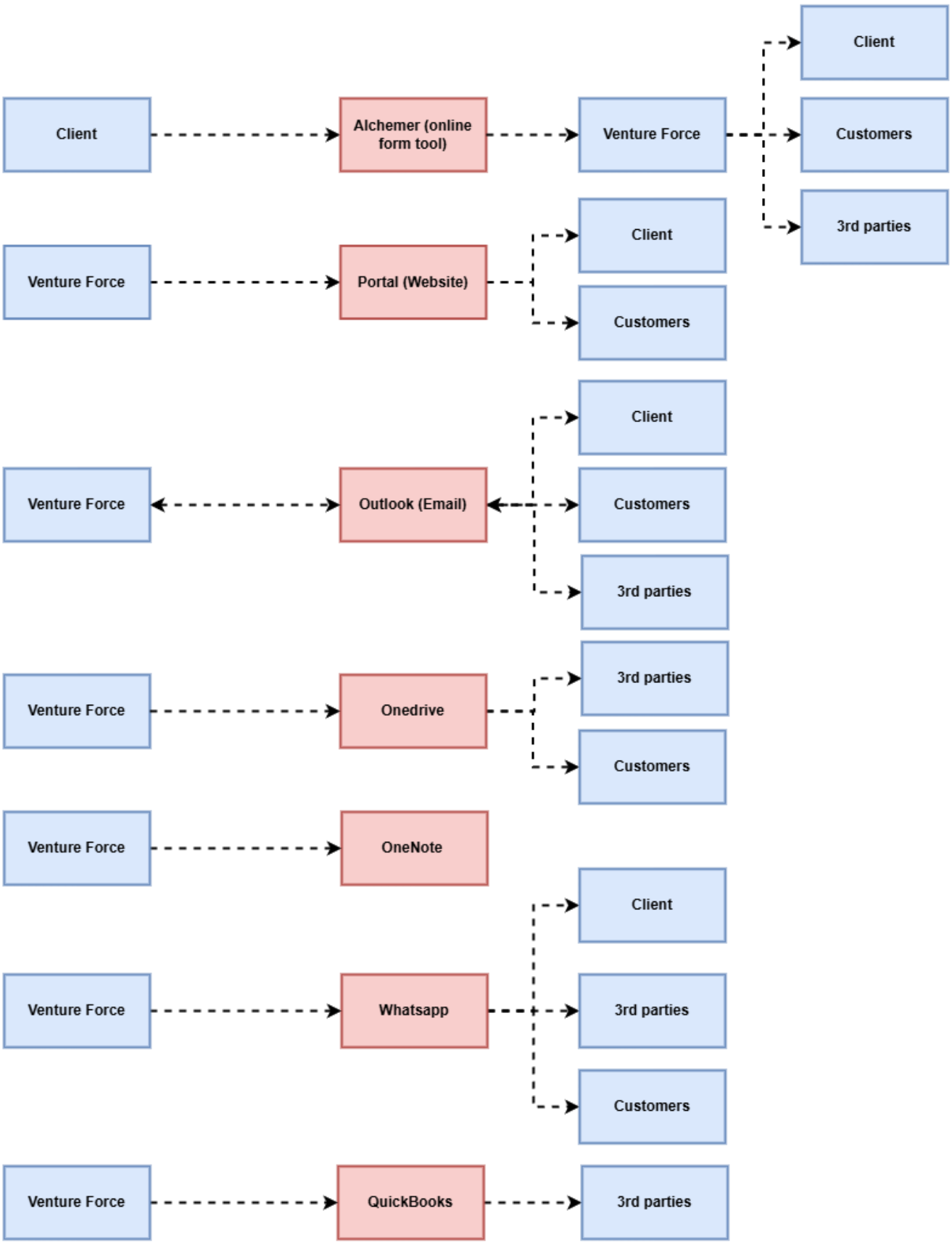
Venture Force uses a range of secure platforms to store and manage personal and sensitive information. These platforms are selected for their ability to support compliance with GDPR and the Data Protection Act 2018, and their use is governed by the controls set out in our Information Security Policy.

Platform	Purpose	Security Measures
Alchemer	Collects personal data from clients via online forms	Data is transmitted securely via SSL (https). Only authorised VF staff have access to the platform.
Avast for Business	Antivirus, firewall, and endpoint protection on VF devices	Provides real-time threat detection, email security, and firewall protection. Managed centrally and monitored.
Company Laptops	Used by VF staff to access systems, records, and communications	All devices are encrypted, password-protected, and installed with endpoint protection. Auto-locking is enforced.
Microsoft 365 (OneDrive, OneNote)	Internal data storage, document sharing, and team collaboration	Files are encrypted at rest and in transit. Access is restricted by job role. External sharing is password-protected.
Mobile Devices (Work Phones)	Used by staff for expedition operations and communication	Devices are password-protected and kept updated. Only used for work purposes. Loss or theft must be reported immediately.*

Outlook (Microsoft Exchange)	Email communication with clients, customers, and third parties	Secure accounts with multi-factor authentication. Data is encrypted in transit and monitored for threats.
Physical Documents	Occasionally used for expedition or HR purposes	Access restricted to authorised staff. Stored securely and shredded after the retention period ends.
Portal / Website (WordPress CMS)	Shares expedition information and resources with clients/customers	Hosted on WordPress and protected by SSL encryption (https). Regular updates and plugin maintenance are applied. View-only access for external users. No personal data is submitted via the portal.
QuickBooks	Manages financial data and customer invoicing	Cloud-based and encrypted. Access limited to VF staff and external accountant under a data processing agreement.
WhatsApp	Used for operational messaging, including team group chats, medical support communications, and document sharing with in-country agents	End-to-end encryption enabled. Groups with members who are customer/participants/agents/expedition leaders are managed by VF staff. Participants are instructed not to share sensitive personal data. Shared documents are reviewed for appropriateness and, where required, are password protected. Groups to facilitate expedition leader communication with medical personnel during expeditions are managed by external medical providers.

*Note: Company Directors are permitted to use their mobile devices for personal use. They must still comply with all relevant data protection and security protocols, and ensure any personal use does not compromise the integrity or security of expedition or client data.

DATA PROCESSING AND STORAGE DIAGRAM



ANNEX ONE

SUMMARY OF DATA TYPES PROCESSED BY VENTURE FORCE

- **Personal Information**
  - Name, date of birth, gender, and contact details (address, phone number, email)
  - Nationality and passport information
  - Emergency contact and next of kin details
  - Educational and employment background
  - Financial details (e.g. payment history, bank info for staff/contractors)
  - Images (e.g. photographs or video taken during expedition activities)
  - Information about dietary requirements
  - Travel history and visa details
  - Records of correspondence (e.g. emails, call notes, application forms)

- **Sensitive Information**
  - Physical or mental health information (e.g. medical history, medication, health declarations)
  - Contact details for healthcare professionals (e.g. GP or consultant), where provided
  - Religious or philosophical beliefs (where relevant to dietary, welfare, or safeguarding needs)
  - Criminal convictions or offences (e.g. DBS check information for staff and leaders)
  - Racial or ethnic origin (only where disclosed by the individual and relevant to safeguarding or operational planning)
  - Gender identity, where disclosed and relevant for safeguarding or operational planning

HOW DO WE COLLECT DATA?

- Online data collection forms (e.g. Alchemer submissions)
- Customer booking forms and expedition registration documents
- Consent forms and medical declarations
- Expedition and leadership contracts
- Employment contracts and onboarding paperwork
- Parent/guardian information schedules
- Leader applications and update forms
- Staff recruitment and vetting documentation
- Job applications and interview notes
- Email communications (e.g. personal information sent via email)
- Phone communications (e.g. verbal updates recorded by VF staff)
- Feedback forms and post-expedition surveys
- Invoices and financial documentation
- Data shared directly by schools or group leaders on behalf of clients

WHAT DO WE USE THIS DATA FOR?

Operational planning and expedition delivery

- Processing applications and confirming identity
- Recording and updating contact details, including emergency contacts
- Booking flights, accommodation, transport, and other logistics
- Managing visa applications and travel permits
- Conducting pre-departure medical screening and health risk assessments

- Supporting Venture Force leaders to run safe expeditions
- Enabling the VF Operations Room to manage in-country incidents and emergencies
- Coordinating volunteering activities or community project placements (where applicable)
- Managing customer payments and issuing invoices
- Paying staff, leaders, and contractors

Safety, safeguarding, and suitability

- Assessing an individual's suitability to participate in an expedition or fulfil a specific role
- Supporting safeguarding, risk management, and individual welfare during expedition planning and delivery
- Meeting the requirements of insurers, accreditation bodies, or expedition standards (e.g. BS 8848)

Internal systems and compliance

- Maintaining personnel, HR, and leadership records
- Supporting internal operations, including audits, data analysis, service development, and fraud prevention
- Supporting internal training, supervision, or quality assurance processes
- Responding to complaints, concerns, or incident reports
- Fulfilling legal obligations and responding to official requests (e.g. HMRC, safeguarding authorities)
- Limiting reputational or legal damage to Venture Force in the event of a dispute or risk event

Communication and engagement

- Responding to information requests from clients, customers, and partners
- Contacting stakeholders about current or future Venture Force opportunities, events, or updates (where consent has been given)
- Promoting and marketing Venture Force and its services (with appropriate consent)

WHO DO WE SHARE DATA WITH AND WHAT DO WE SHARE?

Internal and customer personnel and delivery teams

- **Venture Force key staff** (e.g. permanent staff, expedition managers, expedition leaders, operations room) – Full participant details required to plan and manage the expedition and respond to emergencies.
- **Venture Force volunteers** – Name, gender, date of birth, passport details, medical and dietary information, and any other data required for in-country safety and welfare.
- **Medical Advisor** – Name, date of birth, and medical information for pre-departure screening or incident response.
- **School staff/Customer staff involved in expedition delivery** – Name, gender, date of birth, passport details, medical and dietary requirements, and other information required for joint risk and team management.
- **School emergency contact** – Full participant details, provided for escalation in the event of a serious incident.

Expedition support partners and suppliers

- **Flight agents / airlines** – Name, date of birth, gender, passport details, and dietary requirements for ticketing and travel arrangements.
- **Accommodation providers** – Name, gender, date of birth, and passport details as required for rooming or identity verification.
- **Remote medical services** – Name, date of birth, and medical details, if required for advice or emergency care.
- **Insurance company/broker** – Name and expedition destination for insurance registration.

- **National parks, permit authorities, or visa processing agents** – Name, date of birth, gender, and passport details for access or travel approvals.

Clients' families and representatives

- **Next of kin / emergency contacts** – Shared only when relevant for medical or welfare incidents.
- **Other parents/guardians** – Participant names may be shared for ATOL certificates or expedition confirmation purposes (where necessary).

External professional and regulatory bodies

- **Statutory bodies** (e.g. HMRC, safeguarding authorities, police) – Data shared only where legally required.
- **Business associates and professional advisers** – e.g. HR, legal, or IT consultants, under appropriate confidentiality agreements.
- **Survey or research organisations** – Limited, anonymised or summarised data, unless explicit consent has been given.

ANNEX TWO

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 - Any information that identifies someone as an individual. This may include, but is not limited to:

- Personal details (e.g. name, date of birth, address)
- Family details
- Lifestyle and social circumstances
- Financial information
- Education and employment details
- Visual images

Sensitive personal information is information about an individual's

- Physical or mental health details
- Racial or ethnic origin
- Religious or philosophical beliefs
- Offences and alleged offences
- Criminal proceedings, outcomes and sentences

Key staff - Defined as the Directors, permanent employees, expedition managers, expedition leaders, operations room staff, medical advisor and in-country agents.

Client – The participant in the expedition. In the case of a participant under the age of 18, this term includes the individual and any adult with parental responsibility for them.

Customer – The individual or organisation that has booked the expedition with Venture Force.