VERI-FY IDENTITY LIMITED - PRIVACY POLICY 2018 TABLE OF CONTENTS

1. POLICY STATEMENT

1.1 Everyone has rights with regard to the way in which their personal data in handled. During the course of our activities we will collect, store and process personal data about our members, suppliers and other third parties, and we recognise that the correct and lawful treatment of this data will maintain confidence in the organisation and will provide for successful business operations.

1.2 Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action.

2. ABOUT THIS POLICY

2.1 The types of personal data that Veri-fy Identity Limited (We) may be required to handle include information about current, past and prospective members and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 2018 (the Act) the General Data Protection Regulation 2016 (GDPR) Data Protection Act 1988 and other legislation and regulation.

2.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

2.5 The Data Protection Officer is responsible for ensuring compliance with the Act and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer.

3. DEFINITION OF DATA PROTECTION TERMS

3.1 **Data** is information which is stored electronically, on a computer, or in certain paper-based filing systems.

3.2 **Data subjects** for the purpose of this policy include all living individuals about whom we holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

3.3 **Personal data** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

3.4 **Data controllers** are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own commercial purposes.

3.5 **Data users** are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

3.6 **Data processors** include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

3.7 **Processing** is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

3.8 **Sensitive personal data** (or **special categories of data** under GDPR) includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, genetic data and biometric data

where they are processed in order to uniquely identify a person or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

4. DATA PROTECTION PRINCIPLES

4.1 Anyone processing personal data must comply with the eight enforceable principles of good practice under the DPA – under GDPR these are the following seven, with the DPA principle in relation to the transfer of data being a separate right set out in paragraph 14 of this Policy. These provide that personal data must be (with further detail set out within this Policy):

(a) Processed fairly transparently and lawfully, with consent.

(i) Consent has to be specific, informed and unambiguous indication of an individual's wishes and it can be given by a statement or by a clear affirmative action

(ii) Note significant grounds for processing under the GDPR without specific consent:

(A) in connection with the performance of a contract or

(B) where processing is undertaken in order to comply with a legal obligation

(C) when a data controller can justify data processing on the basis of pursuing its or the company's legitimate interests

(iii) If the consent element is within a document covering other elements, the request for consent must be presented in a form that is distinguishable from the rest of the document and is formulated in clear and plain language

(b) Processed for limited purposes which are explicit and legitimate and in an appropriate way.

(c) Adequate, relevant and limited to the required purposes.

(d) Accurate and up to date.

(e) Not kept longer than necessary for the purpose, with means developed to delete data.

(f) Processed in line with data subjects' rights.

(g) Secure; to monitor this we have a Technology and Security Group meeting monthly and reporting to the Board

4.2 In addition there are specific rights embodied in the GDPR:

(a) Right to be informed of the processing of information, and that the processing is fair; providing an external privacy notice which is concise, transparent, intelligible, easily accessible

(b) Right of Access – under GDPR no charge can be made for this, and information has to be provided within one month of request.

(c) Right of Rectification – under GDPR, within one month of request.

(d) Right of erasure of data where there is not a legitimate reason for it being processed (note: this is not a "right to be forgotten")

(e) Right to restrict processing (note: this means data could still be stored – this may be temporary e.g. whilst investigating)

(f) Right to data portability – to be able to obtain and re-use personal data, in a structured, machine readable and common format e.g. as CSV file; this must be provided within a month of request.

(g) Right to object to data being processed:

(i) If subject objects to reasons for processing

(ii) If processing is for direct marketing - *Privacy and Electronic Communications Directive (2002/58/EC)* requires an individual's prior consent for electronic direct marketing such as email or text

(h) Rights not to be subject to automatic decision making and profiling

5. ACCOUNTABILITY TRANSPARENCY AND GOVERNANCE

5.1 GDPR sets out a requirement of Accountability which is central to this Policy.

5.2 The Company must be able to demonstrate compliance by:

(a) Organisational measures, to include:

(i) Tailored Policies

(ii) Adherence to approved codes of conduct / certifications

(iii) Training at regular intervals

(iv) Audit of processing activities against the principles; the Company will:

(A) At least annually, review the processing activities actually carried out against those stated in any policy

(B) Consider if any additional activities have been added, or any ceased

(C) Review policies to reflect changes, if any.

5.3 The Company must appoint a DPO or equivalent to

(a) Inform and advise the organisation and its employees

(b) Monitor, advise and train

(c) Be the point of contact with supervisory authorities

The DPO must:

(d) Have the necessary skills, training and resources for the role

(e) Not be able to be dismissed or penalised for conduct of the role

(f) Be at board level, and reporting to the board

5.4 The Company will maintain and keep up to date a register of its policies and activities showing:

(a) Details of the organisation

(b) Details of DPO

(c) Purpose of processing

(d) Categories of individuals whose data is processed

(e) Categories of data processed including any special categories of data

(f) Data Processing Impact Assessment, to cover:

(i) Operations and legitimate interests in processing

(ii) Assessment of risk to individuals

(iii) Measures to assess and manage risk

(g) Recipients of data

(h) Third countries to which data is transferred

(i) Retention policy and schedule for data deletion

(j) Technical and organisational security measures

(k) Data Protection by design measures

(l) Training

(m) Breaches

6. FAIR AND LAWFUL PROCESSING

6.1 The Act and GDPR have special categories of data is not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

6.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the Act. These include, among other things, the data subject's consent to the processing, or that the processing is necessary for the performance of a contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, or for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, additional conditions must be met. When processing

personal data as data controllers in the course of our business, we will ensure that those requirements are met.

7. PROCESSING FOR LIMITED PURPOSES

7.1 In the course of our business, we may collect and process the personal data set out in the Schedule 1. This may include data we receive directly from a data subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and data we receive from other sources (including, for example, business partners, sub-contractors in technical, payment and delivery services, credit reference agencies and others).

7.2 We will only process personal data for the specific purposes set out in the Schedule 1 or for any other purposes specifically permitted by the Act or GDPR. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

8. NOTIFYING DATA SUBJECTS

8.1 If we collect personal data directly from data subjects, we will inform them about:

(a) The purpose or purposes for which we intend to process that personal data.

(b) The types of third parties, if any, with which we will share or to which we will disclose that personal data.

(c) The means, if any, with which data subjects can limit our use and disclosure of their personal data.

8.2 If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

8.3 We will also inform data subjects whose personal data we process that we are the data controller with regard to that data, and who the Data Protection Officer is.

9. ADEQUATE, RELEVANT AND NON-EXCESSIVE PROCESSING

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

10. ACCURATE DATA

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

11. TIMELY PROCESSING

We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required.

12. PROCESSING IN LINE WITH DATA SUBJECT'S RIGHTS

12.1 We will process all personal data in line with data subjects' rights, in particular their right to:

(a) Request access to any data held about them by a data controller (see also clause 16).

(b) Prevent the processing of their data for direct-marketing purposes.

(c) Ask to have inaccurate data amended (see also clause 10).

(d) Prevent processing that is likely to cause damage or distress to themselves or anyone else.

13. DATA SECURITY

13.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

13.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

13.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

(a) **Confidentiality** means that only people who are authorised to use the data can access it.

(b) **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

(c) **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on the [COMPANY'S] central computer system instead of individual PCs.

13.4 Security procedures include:

(a) **Entry controls.** Any stranger seen in entry-controlled areas should be reported.

(b) **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

(c) **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

(d) **Equipment.** Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

14. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

14.1 We may transfer any personal data we hold to a country outside the European Economic Area ("EEA"), provided that one of the following conditions applies:

(a) The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.

(b) The data subject has given his consent.

(c) The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.

(d) The transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.

(e) The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

14.2 Subject to the requirements in clause 13.1 above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. That staff maybe engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

15. DISCLOSURE AND SHARING OF PERSONAL INFORMATION

15.1 We may share personal data we hold with any member of our group, which means our subsidiaries (if any), our ultimate holding company (if any) and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

15.2 We may also disclose personal data we hold to third parties:

(a) In the event that we sell or buy any business or assets, in which case we may disclose personal data we hold to the prospective seller or buyer of such business or assets.

(b) If we or substantially all of our assets are acquired by a third party, in which case personal data we hold will be one of the transferred assets.

15.3 If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, members, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

15.4 We may also share personal data we hold with selected third parties for the purposes set out in the Schedule 1.

16. DEALING WITH SUBJECT ACCESS REQUESTS

16.1 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the Data Protection Officer immediately.

16.2 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

(a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

(b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.

16.3 Our employees will refer a request to the data Protection Officer for assistance in difficult situations. Employees should not be bullied into disclosing personal information.

16.4 Subject Access requests must be responded to within one month under GDPR

17. REPORTING BREACHES

17.1 The Company has a duty to report:

(a) Destruction

(b) Loss

(c) Alteration

(d) Unauthorised disclosure of or access to personal data

If the breach is likely to lead to risk to the rights or freedoms of individuals

17.2 The duty is to notify

(a) the ICO

(b) the individuals affected

17.3 Notification must be given within 72 hours

18. CHANGES TO THIS POLICY

We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail or email.

SCHEDULE 1 - Data processing activities

PART 1

Definition of terms for the purposes of this schedule :

"Applicant" – A person who has been request to or opted to have their identity confirmed by using the Company's system.

"Employer" – A person or organisation who has asked an applicant to have their identity confirmed using the Company's system

Note: The Applicant may be employed by or be a volunteer of the Employer

"ID Checker" – A person selected by the applicant to confirm their identity

"DBS Disclosure" - A disclosure issued by the Disclosure and Barring Service in England and Wales and Disclosure Scotland

Type of data	**Type of data subject**	**Type of processing**	**Purpose of processing**	**Type of recipient to whom personal data is transferred**	**Retention period**
Applicant's Personal details excluding financial and sensitive data	Applicant	Creation of template forms	ID confirmation in support of an application for a DBS Disclosure Invoicing	Applicant's employer	Applicant's full name 6 years All other details 14 days
ID Checker's	ID checker	Completion of template	ID confirmation	Applicant's employer	ID Checker's full name and

details excluding financial and sensitive data		form	in support of an application for a DBS Disclosure Invoicing		occupation 6 years No other details retained
Employee financial data	Employee	HR recording for employees	Payroll, Health & Safety , training	Government and Regulatory authorities	Employee information to be retained for minimum of 7 years
Employee HR data	Employee	HR recording for employees	Payroll, Health & Safety , training		Employee information to be retained for minimum of 7 years
Employee family data	Employee	HR recording for employees	Payroll, Health & Safety , training		Employee information to be retained for minimum of 7 years
Employee contact data	Employee	HR recording for employees	Payroll, Health & Safety , training		Employee information to be retained for minimum of 7 years
Former Employees	Employee	HR recording for employees	Payroll, Health & Safety , training		Employee information to be retained for minimum of 7 years

Suppliers					