INVICTUS
Wellbeing Services
Community Interest Company

INVICTUS WELLBEING SERVICES COMMUNITY INTEREST COMPANY

Data Protection Policy

1 Policy statement

1.1 Everyone has rights with regard to the way in which their personal data is handled. During the course of its activities Invictus Wellbeing Services ("Invictus") will collect, store and process personal data (both paper based and electronic) about the schools it services, advisers, suppliers and other third parties, and it recognises 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 behalf of Invictus.

1.3 Invictus also holds and processes personal data for a wide range of purposes, including:

- purchase and supplier information;
- charity & voluntary organisation objectives;
- wellbeing advice administration;
- education and training administration; and
- adviser administration

1.4 This policy and any other documents referred to in it sets out the way in which Invictus will process any personal data that it collects from data subjects, or that is provided to Invictus by data subjects or other sources.

1.5 This policy sets out rules on data protection and a summary of the legal conditions that must be satisfied when Invictus obtains, handles, processes, transfers and stores personal data.

2 Data Protection Officer

2.1 Invictus has appointed the Directors of Invictus as the Data Protection Officers ("DPO") who will endeavour to ensure that all personal data is processed in compliance with this policy and the principles of the General Data Protection Regulation ("GDPR"). This includes ensuring that data is kept securely and not made available to unauthorised parties. The DPO have overall responsibility for compliance with the GDPR and this policy.

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 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 GDPR. Invictus is the data controller of all personal data used in its business for its own purposes.

3.3 **Data users** are those self-employed advisers, directors and any employees of Invictus whose work involves processing personal data. Data users must at all times protect the data that they handle in accordance with this policy and any applicable data security procedures.

3.4 **Data Processors** include any person or organisation that processes personal data on behalf of Invictus and on its instructions. This could include suppliers which handle personal data on behalf of Invictus.

3.5 **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.

3.6 **Data subjects** are living individuals about whom Invictus 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 data.

3.7 **Personal data** is data relating to a living individual who can be identified from that data (or from that data and other information in the possession of Invictus). It includes information that is factual, such as information necessary for self-employed advisers (adviser name and address and details for payment of invoices), but it can also be an opinion about that person, their actions or behaviour.

3.8 **Special Categories of Personal Data** (referred to in this policy as sensitive personal data) is information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

4 Processing of personal data

4.1 Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

4.2 You may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly and without adversely affecting the data subject.

4.3 The GDPR allows Processing for specific purposes, some of which are set out below:

- the Data Subject has given his or her Consent;
- the Processing is necessary for the performance of a contract with the Data Subject;

- to meet our legal compliance obligations;

- to protect the Data Subject's vital interests;

- to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices

5 The principles

5.1 Invictus shall, so far as is reasonably practicable, comply with the legislation and the principles contained within it to ensure that all data is:

- processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
- collected only for specified, explicit and legitimate purposes (Purpose Limitation).
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation).
- accurate and where necessary kept up to date (Accuracy).
- not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation).
- processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
- not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
- made available to data subjects and data subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

6 Fair and lawful processing

6.1 For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the performance of the contract with the data subject, for the compliance with a legal obligation to which the data controller is subject, to protect the vital interests of a data subject or another person or for the legitimate interests of the data controller or the party to whom data is disclosed.

7 Processing for limited purposes

7.1 Personal data may only be processed for the specific purposes notified to the data subject when data was first collected or for any other purposes specifically permitted by the GDPR. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which data is processed, the data subject must be informed of the new

purpose before any processing occurs and/or if necessary fresh consent should be obtained.

8 Notifying data subjects

8.1 If Invictus collects personal data directly from data subjects, it will inform them of:

- the purpose or purposes for which Invictus intends to process that personal data;
- the types of third parties, if any, with which Invictus will share or to which it will disclose that personal data; and
- the means, if any, with which data subjects can limit Invictus use and disclosure of their personal data.

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

8.3 Invictus will inform data subjects whose personal data it processes that it is the data controller with regard to that data.

9 Accurate data

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

10 Timely processing

10.1 Personal data should not be kept longer than necessary for the purpose. This means that data will be destroyed or erased from Invictus systems when it is no longer required.

11 Processing in line with data subjects' rights

11.1 Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw consent to processing at any time;
- receive certain information about the data controller's processing activities;
- request access to their personal data that we hold;
- prevent our use of their personal data for direct marketing purposes;
- ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- object to decisions based solely on automated processing, including profiling;
- prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- be notified of a personal data breach which is likely to result in high risk to

their rights and freedoms;

- make a complaint to the supervisory authority; and in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

11.2 There are certain records which are exempt from the rights of access and these include those relating to references given and sought in confidence by Invictus for the purposes of education, training or employment. Also exempt are certain medical or counsellor records relating to both students, advisers and any members of staff.

12 Data security and Accountability

12.1 Invictus takes the responsibility for complying with the GDPR at the highest management level and will process all personal data that it holds in accordance with this policy.

12.2 Invictus 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 the data processor agrees to comply with those procedures and policies, or if they put in place adequate measures.

12.3 Invictus will maintain data security by protecting the confidentiality, integrity and availability of the personal data, as follows:

- **confidentiality** means that only people who are authorised to use the data can access it;
- **integrity** means that personal data should be accurate and suitable for the purpose for which it is processed;
- **availability** means that authorised users should be able to access the data if they need it for authorised purposes.
- **methods of disposal -** paper documents should be shredded and digital storage devices should be physically destroyed when they are no longer required;
- **equipment -** data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC/laptop when it is left unattended.

13 Notification of Personal data breaches

Invictus will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of Invictus becoming aware of it and may be reported in more than one instalment. Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual. If the breach is sufficient to warrant notification to the public, Invictus will do so without undue delay.

14 Exemptions

14.1 Certain data is exempted from the provisions of the GDPR in the following situations:

- the prevention or detection of crime;

- the assessment of any tax or duty; and
- where the processing is necessary to exercise a right or obligation conferred or imposed by law upon Invictus.

14.2 The above are examples of some of the exemptions under the GDPR.

December 2018