Data Protection Policy

1. Introduction

1.1 In order to operate our business, Triangle Consulting Social Enterprise Ltd ("Triangle") needs to collect, store, share and use certain types of information about its staff, its customers, service providers and the organisations and people who use its web-based application, the Star Online as under www.staronline.org.uk ("Star Online").

1.2 Personal Information means information about staff (see Section 3), Star Online Client Details (see Section 4), and collaborators, clients and potential clients (see Section 5). It is obtained directly from individuals and, when appropriate, from third parties. This information may include contact details, financial information and sensitive and non-sensitive personal information. Potentially sensitive information includes information about race or ethnicity, health, age and involvement in criminal activity. The information may be held and used in paper and other electronic formats.

1.3 Triangle will use all personal information correctly and lawfully. This is a fundamental principle of our work with our clients. It is central to our successful operation and to maintaining the confidence of those with whom we work. Triangle and its staff, associates and contractors respect the privacy of all personal information, and ensure it is treated fairly, lawfully, correctly and confidentially.

1.4 Triangle's directors are aware of policies and procedures to comply with the GDPR, in particular the data protection principles, and maintain direct regular contact with the Business Manager about this aspect of the business.

2. General Data Protection Act (GDPR)

2.1 Triangle complies with the General Data Protection Act effective as of 25th May 2018 (GDPR) and any subsequent applicable data protection legislation. The GDPR does not apply to information held about organisations or to anonymous information (e.g. statistics). It does apply to all personal information held about living people including named contacts within an organisation. It applies to both electronic and hard copy information.

2.2 All personal information held by Triangle is collected, held and used in accordance with the principles of the GDPR. It is:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

2.3 In addition, Triangle ensures that:

- Triangle employees, associates and contractors who manage and use personal information understand that they are responsible for complying with the law and applying good data protection practice;
- Everyone in Triangle who manages and uses personal information is appropriately supervised and trained to do so;
- Everyone who manages, uses or accesses personal information on behalf of Triangle (such as associates, contractors, in particular managing and technical support of the Star Online) abides by the GDPR and is bound by the terms of a confidentiality agreement;
- Methods of using personal information are clearly specified;
- Anyone wanting to make enquiries about the handling of personal information is told what to do and whom to approach;
- The Business Manager and the directors regularly review how personal information is managed and used within Triangle and carry out any necessary updates to policy, processes or staff training.

2.4 Triangle is registered as a Data Controller for the purposes of the GDPR under registration number ZA069260 and as such responsible for compliance with the principles listed under 2.2. Triangle's Business Manager, responsible for implementation of Triangle's data protection and confidentiality policy, is Angela Kallabis, The Dock Hub, Wilbury Villas, Hove BN3 6AH, United Kingdom. An employee or other data subject (an individual who has information held on them within Triangle) who wishes to raise concerns or queries about the holding and processing of personal data should contact the Business Manager.

2.5 **Lead supervisory authority –** As Triangle's intellectual property and products are used in other EU countries, Triangle determines that the UK Information Commissioner's Office (ICO) is the lead supervisory authority.

2.6 **Freedom of Information –** Triangle is not a Public Authority, is not subject to the UK Freedom of Information (FOI) Act and is not responsible for holding statutory information subject to the provisions of the FOI. Triangle staff must not release information in response to requests for information under the Act. Triangle will, however, cooperate in a timely fashion with its clients who may be subject to the FOI Act to satisfy any requests in relation to their business. Any such requests should be referred to the Business Manager.

3. Data on job applicants, employees, associates and contractors

3.1 Triangle holds and processes data relating to employment or other working relationships (for example associates or contractors) ("Staff and Contractor Details"). Such data is confined to that which is necessary to ensure that we have adequate records for employment and contractor related purposes, to meet our legal obligations. This may include all or some of the data relating to:

- Names, addresses, telephone numbers, date of birth, passport, national insurance and bank details as well as information on education and work experience.
- Job applications, employment records, disciplinary and performance records, pay details, expenses, employment benefits, statutory entitlements, qualifications and training, health and safety and employment related insurance;

- Sickness and absence records, including medical records/reports, accident reports and matters relating to fitness for work;
- Information about members of pension schemes for Triangle staff during employment and after retirement;
- Criminal convictions – where these are not regarded as spent in accordance with the Rehabilitation of Offenders Act 1974, or where the post is exempt from the legislation;
- Monitoring employment trends including equal opportunities data and statistics.

3.2 **Lawful basis:** The lawful basis for the collection and processing of information of employees, associates and contractors is Contract.
The lawful basis for the collection and processing of information of job applicants is Consent, which provides the individuals with the right to erasure, portability and to withdraw consent.

3.3 From time to time Triangle may transfer Staff and Contractor Details within the organisation. There may also be occasions when Staff and Contractor Details are passed to other organisations working with Triangle in providing employment related services such as payroll, accountancy, pensions and other benefits, insurance, training, partnership or consultancy projects and so on. In addition, Staff and Contractor Details may be used for the provision of references or other purposes, including to government departments (for example the Inland Revenue) or other bodies to meet our legal obligations. A consent form is given to staff, and an information letter sent to associates, informing them of the details how their information is shared.

3.4 When we request information from potential and existing employees, volunteers and other workers (e.g. job application forms and payroll information forms) we will specify the purposes for which the information is being held and processed and seek consent from the individual in line with the requirements of the GDPR, ie consent will be specific, granular (where appropriate), clear, prominent, opt-in, documented and easily withdrawn.

4. Data kept on the Star Online about staff and service users of our customer organisations

4.1 Triangle's Privacy notice for users of the Star Online system sets out how we look after the information of customer staff and service users of our customer organisations and is available on Triangle's website.

4.2 The lawful bases for our customers, including prospective customers, is Contract.

The lawful bases for the service users of our customers is Legitimate Interests, as we process service user data to fulfil our contractual obligations and do not have a direct relationship with service users.

5. Data on collaborators, customers and prospective customers

5.1 Triangle's Privacy notice for customers details how we look after their information and is available on our website. This applies to existing or prospective customers ("Customers") as well as those organisations or individuals who have expressed interest or support to collaborate with us ("Collaborators").

5.2 The lawful basis for the collection and processing of information for Customers and Collaborators is Contract.

The lawful basis for subscribers to our mailing lists for marketing purposes, whether they are customers or not, is Consent.

6. GDPR declarations, consent for personal information collection, information transfer and future marketing

6.1 Where Triangle requests sensitive personal information (including equal opportunities information, criminal records and health details) from individuals, whether they are job applicants, employees, volunteers or others, Triangle will include wording describing the exact purpose for doing so, how long Triangle wishes to hold the information, how it will be used and with whom it may be shared.

6.2 Where Triangle wishes to hold and use data for marketing and/or to follow up with clients or other contacts and provide further information, Triangle will seek their consent and the clearly worded option to unsubscribe from future communications.

7. eSecurity responsibilities of managers and staff

7.1 The Managers will ensure that staff are aware of the high risk to confidentiality involved when taking information off site. Triangle will ensure any information that is needed off site is kept to a minimum.

7.2 All confidential information held electronically, including all information relating to job applicants, staff, associates and Star Online Client Details are stored on secure servers and drives. Where it is absolutely necessary for personal information to be stored on transportable electronic media appropriate measures will be taken to protect it.

7.3 All computers are protected with a complex password. Staff will log out whenever they are away from their desks, set it to go to sleep after 10 minutes and to require the password to start it again.

7.4 Triangle staff store personal information on a secure, password-protected file sharing system, rather than their laptop or PC hard drives, which provides automatic back-up.

7.5 Mobile devices (such as mobile phones or other devices such as tablets and laptops) that store personal data whether owned by Triangle or an individual staff member, must comply with the following security measures:

- A screen lock (may be known by other names on different devices) must be implemented to require a password or code to be entered after being idle for a maximum of 5 minutes.
- Staff members must not use the default passwords provided by their phone or voicemail service, but must create a new one.
- The mobile phone passphrase or passcode must not be disclosed to anyone.
- When sharing mobile devices, staff members must ensure that applications holding personal data (such as file-sharing apps) are not accessible by others.

7.6 When transferring personal or sensitive information to someone else to carry out their duties, staff, contractors and associates will save the information to an appropriate folder on Triangle's file-sharing system, which has password-protected access (currently Dropbox) or password protect the file before emailing it.

7.7 Information is usually transferred between offices electronically. Situations where staff take paper based personal information from one office base to another, should be avoided unless there is a compelling case for this to happen.

7.8 Except in exceptional circumstances, highly confidential information should always be hand-delivered to the individual concerned rather than being sent by post. Where posting documents is the only option, information should be sent securely by recorded delivery.

7.9 Filing cabinets containing personal information are closed and locked whenever the room is vacated by staff with the right of access to the information. Staff and visitors without the right of access to information are not left unattended in any room with unsecured personal information.

7.10 Desks are cleared of all personal information whenever the room is vacated, unless the room can be locked.

7.11 When personal information is no longer needed, it will be destroyed in the appropriate way. For printed information, it will be shredded, put in confidential waste bags, or ripped up. For electronic information, it will be permanently deleted from all locations where it is stored, including in emails and on servers.

8. Breaches

8.1 Any breaches or possible breaches of information security are reported immediately and verbally, as well as in writing, either directly to a Director or the Data Protection Officer, or the line manager who will share the breach with the Data Protection Officer.

8.2 Any breach of information security practices by staff, associates or contractors will be treated very seriously and action will be taken as appropriate, including through disciplinary procedures where applicable.

8.3 The Data Protection Officer will also decide together with the responsible Director if the breach needs to be reported to the ICO and the individual(s) involved informed.

9. Individuals' rights

9.1 Triangle will communicate the reason for collecting information on individuals, how it is shared and how long it is held for, and will inform individuals' about their rights at the moment when we collect the information in line with the GDPR requirements.

9.2 Under the GDPR individuals have a right of access to personal information held about them, with the exception of information concerning a third party.

Where information does relate to a third party (e.g. confidential employment references) the manager responsible for holding the information should consider whether it is reasonable to disclose the information or whether disclosure could amount to a breach of confidentiality in relation to the provider of the reference.

9.3 If an employee, associate, contractor, collaborator or client wishes to access their file they should make a written request to the manager holding the information, specifying whether they wish to view the data or receive a copy of the information held. The information requested or viewing access will be granted within 30 days of the request being received.

9.4 An individual has the right to be sent their information in a common format, request that incorrect information be corrected, or that inaccurate or irrelevant information be removed. Any such request must be made in writing to either the manager concerned, the Business Manager or one of the Directors. He or she will consider the request and respond to the individual. If there is any disagreement, the Business Manager should be consulted and then, if there is still disagreement, one of the directors. Triangle reserves the right under the Act to refuse repeated requests to access personal information unless they are made at reasonable intervals.

10. Retention of data

10.1 The categories of information which Triangle will hold and the time for which we will normally hold it will be as follows in accordance with legal advice and the Code of Practice published by the Office of the Information Commissioner:

Type of Record	**Maximum Duration**	**Owner**
Details of collaborators, clients or potential clients	5 years after last contact	Business Manager
Contracts and agreements	12 years after termination of the contract	Business Manager and Finance
Complaints from clients	5 years after termination of the contract	Director of Operations
Tax, payroll and pensions information, payments, bank statements and counterfoils, ledgers, receipts and invoices	7 years	HR and finance
Board minutes, corporate governance documents, investments, fixed assets and annual accounts	Indefinite	Directors
Unsuccessful job applications	1 year except where explicit permission given to retain them for future opportunities	HR
Personnel records held by HR	7 years from end of employment	HR
Details of pensioners	7 years from end of pension benefit	HR
Deeds of covenants, leases, building work and planning permissions	12 years after interest in the property has ceased	Business Manager
Accident reports	Indefinite	HR