Data Protection Policy

The organisation is committed to being transparent about how it collects and uses the personal data of its employees, applicants, partners, consultants, clients, colleagues and all contacts to meet its data protection obligations. This policy sets out the organisation's commitment to data protection, and individual rights and obligations in relation to personal data Under the General Data Protection Regulation 2018 (GDPR).

This policy applies to the personal data of employees, applicants, partners, consultants, clients, colleagues and all contacts, referred to as HR-related personal data.

The organisation has appointed Scott Chapman and Cath Ferris, as the persons with responsibility for data protection compliance within the organisation. They can be contacted at ap@southcoastnetwork.co.uk. Questions about this policy, or requests for further information, should be directed to them.

The procedures and principles set out in this policy must be followed at all times by the organisation, its employees, agents, contractors, or other third parties working on behalf of the company. Any employee who fails to observe this policy may face disciplinary action under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice. Any non-employee who breaches this policy may have their contract terminated with immediate effect.

Definitions
“Data subject” is a living individual to whom personal data relates.
"Personal data" is any information that relates to a data subject who can be identified from that information. Processing is any use that is made of data, including collecting, storing, amending, disclosing or destroying it.
"Special categories of personal data" means information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation and biometric data.
"Criminal records data" means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

Data protection principles
The organisation processes HR-related personal data in accordance with the following data protection principles:

- The organisation processes personal data lawfully, fairly and in a transparent manner.
- The organisation collects personal data only for specified, explicit and legitimate purposes.
- The organisation processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- The organisation keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- The organisation keeps personal data only for the period necessary for processing.

- The organisation adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The organisation tells individuals the reasons for processing their personal data, how it uses such Data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons. Where the organisation relies on its legitimate interests as the basis for processing data, it will carry out an assessment to ensure that those interests are not overridden by the rights and freedoms of individuals.

Where the organisation processes special categories of personal data or criminal records data to perform obligations or to exercise rights in employment law, this is done in accordance with a policy on special categories of data and criminal records data. The organisation will update HR-related personal data promptly if an individual advises that his/her/their information has changed or is inaccurate.

Personal data gathered during the employment, worker, contractor or volunteer relationship, or apprenticeship or internship is held in the individual's file (in hard copy or electronic format, or both).

The organisation keeps a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the GDPR.

Lawful, Fair, and Transparent Data Processing
The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
- The processing is necessary for compliance with a legal obligation to which the data controller is subject;
- The processing is necessary to protect the vital interests of the data subject or of another natural person;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the personal data in question is in the Special Categories of Personal Data, at least one of the following conditions must be met:

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);

- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
- The processing relates to personal data which is clearly made public by the data subject;
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
- The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Individual rights
As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests
Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;

- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and
- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. To make a subject access request, the individual should send the request in writing to Scott Chapman or Cath Ferrisor to ap@southcoastnetwork.co.uk. In some cases, the organisation may need to ask for proof of identification before the request can be processed. The organisation will inform the individual if it needs to verify their identity and the documents it requires.

The organisation does not normally charge a fee for the handling of subject access requests. The organisation will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the organisation processes large amounts of the individual's data, it may respond within three months of the date the request is received. The organisation will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the organisation is not obliged to comply with it. Alternatively, the organisation can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the organisation has already responded. If an individual submits a request that is unfounded or excessive, the organisation will notify them that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data as follows:

- The right to be informed;
- The right of access;
- The right to rectification;
- The right to erasure (also known as the 'right to be forgotten');
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights with respect to automated decision-making and profiling.

Rectification of Personal Data

Data subjects have the right to require the organisation to rectify any of their HR-related personal data that is inaccurate or incomplete. The organisation shall rectify the HR-related personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the organisation of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

Erasure of Personal Data
Data subjects have the right to request that the organisation erases the HR-related personal data it holds about them in the following circumstances:

- It is no longer necessary for the organisation to hold that HR-related personal data with respect to the purpose(s) for which it was originally collected or processed;
- The data subject wishes to withdraw their consent to the organisation holding and processing their HR-related personal data;
- The data subject objects to the organisation holding and processing their HR-related personal data (and there is no overriding legitimate interest to allow the organisation to continue doing so);
- The HR-related personal data has been processed unlawfully; or
- The HR-related personal data needs to be erased in order for the organisation to comply with a particular legal obligation**.**

Unless the organisation has reasonable grounds to refuse to erase HR-related personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
In the event that any HR-related personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

Restriction of Personal Data Processing
Data subjects may request that the organisation ceases processing the HR-related personal data it holds about them. If a data subject makes such a request, the organisation shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the HR-related personal data in question is not processed further. In the event that any affected HR-related personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

Objections to Personal Data Processing
Data subjects have the right to object to the organisation processing their HR-related personal data based on legitimate interests. Where a data subject objects to the organisation processing their HR-related personal data based on its legitimate interests, the organisation shall cease such processing immediately, unless it can be demonstrated that the organisation's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

Adequate, Relevant, and Limited Data Processing
The organisation will only collect and process HR-related personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

Data Retention

The organisation shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
When HR-related personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay. For full details of the organisation's approach to data retention, including retention periods for specific personal data types held by the organisation, please refer to our Data Register.

Data security
The organisation takes the security of HR-related personal data seriously. The organisation has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Where the organisation engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

Data breaches
If the organisation discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect.
If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

International data transfers
The organisation will not transfer HR-related personal data to countries outside the EEA.

Individual responsibilities
Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes their bank details. Individuals may have access to the personal data of other individuals and of our customers and clients, in the course of their employment, contract, volunteer period, internship, apprenticeship or any other capacity. Where this is the case, the organisation relies on individuals to help meet its data protection obligations to staff customers and clients where the organisation deems appropriate.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;

- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware of to Scott or Cath at email: ap@southcoastnetwork.co.uk immediately.

Training
The organisation will provide training to all individuals about their data protection responsibilities as part of the induction process. Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will have additional training suggested to help them understand their duties and how to comply with them.

This Data Protection Policy is not contractual and may be changed by the Organisation at any time.