careerstudio | CREATIVE CAUSE | Apprenticeships in Scotland | INSPIRING PURPOSE

GDPR

GENERAL DATA PROTECTION POLICY

INTRODUCTION

Career Studio (Scotland) Ltd is a micro business engaged in providing personal career services to individuals, training services to employers, digital media services to a range of business clients and educational programmes to schools and other educational organisations. In addition, we process data for the general administration of our business.

In preparation for GDPR we have undertaken an audit of our business data and conduced a review of our data management processes. In doing so we have considered fully the personal data we ask for, the personal data we process, the personal data we store and the personal data we share for each area of our business.

Career Studio (Scotland) Ltd are registered data controllers with the information commission registration https://ico.org.uk/ESDWebPages/Entry/ZA064492.

CONTENTS

1 PURPOSE

1.1 We collect, store and process information relating to individuals (personal data) whilst carrying out our business activities. This document is necessary to help ensure compliance with our legal obligations in respect of data processing.

1.2 It is also intended to be a key tool toward demonstrating compliance measures to regulators and may be regarded by them as a top layer document and therefore comprises part of our layered approach to documenting practices in this area.

1.3 Through this policy and other practices, the organisation aims to create and operate a culture of openness in respect of data processing.

2 SCOPE

2.1 As an established micro business in the UK, this policy applies to all processing of personal data regardless of where in the world that processing, or any processing outsourced by us may take place.

2.2 This policy applies to Career Studio (Scotland) Limited and the various general business activities undertaken by Career Studio (Scotland) Ltd including 'Career Studio Training and Development Services'; Career Studio Personal Career Services'; 'Apprenticeships in Scotland'; 'Creative Cause'; 'Character Scotland'; Character Development Fund for Scotland'; 'Inspiring Purpose'; 'Association for Character Education' and any other such trading and general business activities which may be generally identifiable as part of the general operation of Career Studio (Scotland) Limited.

2.3 This is an internal policy and it applies to all employees, workers and any other internal persons who may have responsibility for or a vested interest in the operations of the organisation its trading activities.

2.4 The document may be shared with third parties, contractors and other self-employed persons who will be asked to comply with the policy. Where the organisation does undertake the services of a third party, that party will be required to make adequate assurances to the data controller and/or processor and the Data Protection Officer that their own processing is compliant with current applicable data protection laws.

2.5 The policy applies to all data processes in general but particularly to all activities relating to the acquisition, recording, processing, sharing storing and removal of personal data. In respect of carrying out general business activities and for illustrative purposes only, such processes include but are not limited to the personal data we ask for, the personal data we process, the personal data we store and the personal data we share for the purpose of our General Business Activities. For example:

The personal data we ask for may include personal information including personal details, family details, lifestyle and social circumstances, financial details, education, training and employment details. We may also ask for physical or mental health details, racial or ethnic origin, political opinions and religious or other beliefs of a similar nature. We recognise this is highly sensitive personal data and is only asked for by suitably qualified career guidance professional bound by a code of ethics governed by the professional body (Career Development Institute).

The personal data we process enables us to produce curriculum documentations, educational records and awards, training information and other information suitable for educational, training and employment purposes.
The personal data we may store within our confidential client records which are accessible only to the career guidance professional associated with each client. The data is stored as password protected email communication threads and associated attachments. We may store other information relating to education programmes, training or client account information. This data may only be accessed by authorised employees.

the personal data we may share from personal information items listed above with other employment, training and personal development related organisations will only occur with the explicit written consent or instruction of our client and never in breach of client confidentiality as would be within the ethical boundaries for a career development professional.

3 STATEMENT

3.1.1 We are committed to engendering a culture of accountability, integrity and confidentiality in all aspects of the organisation in regard to personal data and security. Our ultimate aim is to align every member of staff to these values such that they may be ambassadors of best practice data processing. We seek to achieve this by inducting new starters into our security practices and to maintain engagement and commitment to these values through transparent communication, providing regular training to staff and embedding privacy into our practices.

3.1.2 As an employer we process personal data about our staff. The type of information we require includes: nationality, date of birth, contact details and medical information. The grounds upon which this information is required will include legal and contractual obligations such as; demonstrating right to work checks, meeting statutory payment conditions and corresponding with individuals in respect of their employment.
3.1.3 Please refer to section the section 'Roles and responsibilities' for the details of the Controller. For a list of your rights as a data subject, please refer to section 'The rights of data subjects'.

4 PRINCIPLES

4.1 All persons who process personal data with our permission must endorse and adhere to these principles at all times and especially when they obtain, handle, process, transfer, store or erase personal data.

4.2 The six fundamental principles of personal data processing are as follows:

1. Fairness, lawfulness and transparency
   All personal data must be processed fairly, lawfully and transparently.
2. Purpose limitation
   All personal data must be collected for specified, explicit and legitimate purposes and shall not be further processed in any manner that is incompatible with those purposes.
3. Minimisation
   All personal data must be adequate, relevant and limited to what is necessary for the purpose for which they are processed.
4. Accuracy
   All personal data must be accurate and where necessary, kept up to date with regards to

the purposes. Every reasonable step to rectify or erase inaccurate personal data must be taken without delay.

5. Storage limitation
   No personal data should ever be kept in a form which permits identification of a data subject for longer than is necessary to achieve the purpose.
6. Integrity and confidentiality
   All personal data must be processed in a manner that ensures appropriate security of the personal data. At the very least, it must always be protected against unauthorised or unlawful processing, accidental loss, destruction or damage, by using appropriate technical and organisational measures.

The data controller is ultimately accountable for each of these principles and is obliged by law to be able to demonstrate compliance at all times. It is for this reason that everyone in the organisation is required to take responsibility for their own strict adherence to these principles.

4.3 This policy is not contractual as it may be subject to change. However, it does indicate how we intend to meet our legal responsibilities for data protection. Therefore, any actionable points within it must be regarded as a legitimate management instruction. Explicit permission must always be sought and evidenced from a line manager before conducting yourself in a manner that varies from this policy. Failure to do so may result in disciplinary action.

4.4 Any additions or revisions to this policy will be communicated to staff where appropriate. We will notify data subjects of any changes that apply to them where appropriate, personally and in writing.

5 DEFINITIONS

5.1 Data
Information which is processed or is intended form part of a filing system. This applies to electronic or hard copy formats.

5.2 Data subject
An identified or identifiable, natural, legal person.

5.3 Data Protection Impact Assessments
A Data Protection Impact Assessment (DPIA) is also known as a Privacy Impact Assessment (PIA). It is a method which may be used to ensure privacy by design by conducting a prescribed risk assessment on data processes and making necessary adaptations, thereby implementing appropriate safeguarding measures. A DPIA is made mandatory by law in certain circumstances.

5.4 Data protection legislation
All privacy laws applicable to any Personal Data processed under or in connection with this Agreement, including, without limitation, the UK Data Protection Act 1998 , the Data Protection Directive 95/46/EC (as the same may be superseded by the General Data Protection Regulation 2016/679 (known as "GDPR"), the Privacy and Electronic Communication Directive 2002/58/EC and all national legislation implementing or supplementing the foregoing and all associated codes of practice and other guidance issued by any applicable Data Protection Authority, all as amended, re-enacted and/or replaced and in force from time to time.

5.5 Personal data (personal information)
Any 'data' relating to a 'data subject' who can be directly or indirectly identified by reference to a piece of data. This includes a name, identification number, location data or online identifier. It may be an identifier that relates to physical, physiological, genetic, mental, economic, cultural or social identity. It may also apply to data that has been pseudonymised.
The nature of the definition of data and personal data means that the expression of opinion or view about a data subject may also be regarded as personal data.

5.5.1 Special category data (sensitive data)
This is also more commonly referred to as 'sensitive data'. In essence this is any data that has the potential to be used to discriminate against a natural person. It includes: racial, ethnic, political opinion, religious or philosophical belief, trade union membership, genetic, biometric data, sex life or sexual orientation data.
It does not include information pertaining to criminal convictions however, such information must be treated with a higher level of security than generic personal data.

5.6 Privacy by design
Privacy by design is the concept of ensuring that security, confidentiality and integrity of personal data is prioritised within the heart of the methods used for processing the data.

5.7 Processing
Any activity which is performed on personal data whether or not this is manual or automated, such as: recording, organising, structuring, storing, updating, retrieving, disclosing or erasing. Examples may include; sorting e-mail addresses into categories for marketing campaigns, recording absences from work, monitoring vehicle tracking etc.

5.8 Pseudonymise
To adapt how personal data is processed and presented such that the data cannot be attributed to a specific data subject, without additional personal data. The additional personal information must be kept separately and securely using appropriate technical and organisational measures.

5.9 Recipient
A natural person or organisation to whom personal data is disclosed or made available to. A recipient is not necessarily a third party with who the Company has professional dealings.

6 ROLES AND RESPONSIBILITIES

Data Controller
The Company's Data Controller is Ronnie Davidson, Career Development Director who may be contacted directly at any time on 01334 844900 Email: ronnie@careerstudio.co.uk.

6.1.1 The role
The Data Controller is the key decision maker in respect of why and how personal data is used and handled. The Data Controller will ensure that, both in the planning and implementation phases of processing activities, data protection principles and appropriate safeguards are addressed and implemented and that records of processing activity are kept. Our Data Controller will ensure that a Privacy Impact Assessment (PIA) is carried out when necessary.

6.1.2 Overview of responsibilities

- To be ultimately accountable for the Company's compliance with the six principles (see section 'Principles').
- To be able to demonstrate compliance with the six principles and therefore the proper handling and processing of all personal data. This will include information about the various data protection management resources that have been put into place and take the primary responsibility for the internal data protection framework.
- To implement appropriate technical and organisational measures to ensure processing is performed in accordance with data protection laws. These measures will take into account the nature, scope, context and purposes of the data processing and the risks to the rights and freedoms of individuals.
- To adopt measures to protect against any high levels of risk identified by a Privacy Impact Assessment, such as; discrimination, identity theft or significant legal, social or economic disadvantage.
- To implement internal data protection policies; assign protection responsibilities and to ensure adequate training on data protection is provided and carried out by all staff.
- To determine how data subjects may exercise their rights.

6.2 Data Processor

6.2.1 The role

This role processes personal data on behalf of and further to documented instruction given by the Controller.

6.2.2 Overview of responsibilities:

- To take all measures required to ensure their own compliance with data protection legislation regarding security.
- To make available all information necessary to demonstrate compliance with data protection legislation and to permit an audit should the Controller wish to further ensure compliance.
- To assist the controller in compliance with its obligations under data protection legislation regarding;
    - security of processing
    - assist in meeting any rights exercised by a data subject e.g. subject access request
    - notification of a personal data breach to the supervisory authority
    - communication of a personal data breach to the data subject
    - any necessary Data Protection Impact Assessments
    - consultation with the supervisory authority about any processing that should be identified as being 'high risk'
- To ensure that on instruction from the Controller, any personal data held on behalf of a client for whom we act as a processor, is deleted and returned to that client, unless we are prohibited by data protection legislation.
- To immediately inform the Controller if it believes any instruction given by the Controller would be in breach of data protection legislation.

Any processors are not permitted to appoint another processor without prior written agreement from the Company. Equally when we act as a processor we will not appoint another processor without written agreement of the Controller we act on behalf of.

7 CONDITIONS FOR PROCESSING DATA

7.1 Under data protection legislation the processing of personal data is prohibited unless there is a legitimate legal basis upon which the data is being processed. There are six potential legal bases for processing.

7.2 All persons authorising the processing of personal data must be assured that at least one of the following bases applies:

7.3 Legal bases for personal data processing

7.3.1 Consent
The data subject must have given consent for specific purposes and be given the option to withdraw consent at any time. Lawful consent may only be obtained if prescribed conditions set out by data protection laws have been met. Consent must always be explicit and may not be implied.

7.3.2 Contract
The processing must be necessary to enter in to or adhere to a contract which the data subject is party to. For example, to enter into a contract of employment or when a product or service is purchased by the data subject and personal data is required to provide or perform it.

7.3.3 Legal obligation
The processing must be necessary to comply with a legal obligation that you are bound to. For example, tax obligations, evidencing the right to work or to ensure compliance with the Working Time Directive etc. Legal obligations imposed by a country outside of the EU may not be justified under this legal basis.

7.3.4 Vital interests
The processing is necessary to protect vital interests of the data subject. For example, subjects who are unable to make decisions in the best interests of their health.

7.3.5 Public interest
The processing is necessary to perform a task either in the public interest or under instruction from an official authority or regulatory body. This must be sufficient to reasonably override the interests and rights of the data subjects concerned. It may be used for the defence of a legal claim.

7.3.6 Legitimate interest
The processing must be necessary to pursue a legitimate interest, except where it is overridden by fundamental rights and freedoms of the data subject. (This is not applicable to public authorities.) It is likely to be appropriate where people's data is used in a way in which they may reasonably expect, with minimum impact to their privacy, or where there is a compelling justification for the processing.

7.4 Special category data
The processing of special category or 'sensitive data' is strictly prohibited under UK and EU data protection laws. There are limited circumstances in which it is permissible to process special category data. If any of the conditions are met, then all other conditions and protections afforded to regular personal data will also apply. Some provisions including security, should be imposed more strictly.

Conditions under which special category data may be processed are:

7.4.1 The data subject has given explicit consent to the processing of personal data for one or more specified purposes, and there is no overriding legal prohibition.

7.4.2 Processing is necessary to carry out obligations and specific rights of the controller or of the data subject in the field of employment, social security and social protection law. Appropriate safeguards are imperative.

7.4.3 Processing is necessary to protect the vital interests of the data subject or of another person who is physically or legally incapable of giving consent. For example, in a medical emergency.

7.4.4 Processing relates to personal data which are obviously made public by the data subject.

7.4.5 Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts make instructions to the Company when acting in their judicial capacity.

7.4.6 Processing is necessary for reasons of substantial public interest, on the basis of data protection legislation. Advice from the relevant supervisory authority may need to be sought in advance to agree the appropriateness of this condition.

7.4.7 Processing is necessary for the purposes of the assessment of the working capacity of the employee

7.5 Criminal convictions and offences

7.6 Personal data of this nature shall be handled with a greater level of protection than that which may be adequate for the processing of standard personal data.

7.6.1 The Company shall only process data of this nature where there is a legitimate requirement to do so, namely in respect of its duties as an employer. Where there is a legal obligation for the Company to review or record data of this nature an appropriate member of staff may seek to establish the required information from the employee, worker, self-employed person, contractor or any other third party.
Examples of when this may be necessary include; when the performance of a duty requires a criminal record check.

7.7 Processing which does not require identification

7.7.1 When processing information, if you can remove all personal data which identifies the data subject, then you will no longer be required to adhere to the conditions for processing detailed in this policy.

7.7.2 If a data subject becomes identifiable then the conditions for processing will apply.

8 COLLECTING DATA

8.1 Transparency principle

Anyone acting on behalf of the company is expressly required to make sure that any information they provide to a data subject or supervisory authority is done so in a manner that is: concise, transparent, intelligible, uses clear and plain language and is provided in an easily accessible form.

8.2 Collecting personal data from the subject

8.2.1 If during the course of your employment you are required to collect personal data, you must ensure that the data subject is advised or made aware of each of the following:

- The identity and contact details of the controller
- The purposes and legal basis of the processing
- If the legal basis is the Company's legitimate interest, the interest must be detailed
- The recipients or categories of recipients of the personal data, if any
- Whether there is an intention to transfer personal data outside the European Economic Area and if so, whether an adequacy decision by the European Commission exists in relation to the transfer, or alternatively reference to the appropriate or suitable safeguards relied upon by the Company and how these can be obtained

To ensure fair and transparent processing, the following information must also be provided to the data subject:

- The length of time the personal data will be stored for or the criteria used to determine the length of time it will be stored for.
- Details of their rights (see section 15).

8.3 Collecting personal data from a source other than the subject

8.3.1 When information of this nature is collected, the subject must be provided with all the information in the above clause as well as the information below. This should be provided at the time it is obtained, in concise and plain language:

- The categories of the personal data collected
- The source of the data (and whether it was publicly available)

8.3.2 In these circumstances, the information must be provided within a reasonable period after obtaining the personal data, but at the latest within one month. However, if the data shall be used to communicate with the subject, then the information must have been provided by the first communication. If it shall be disclosed to another party, then the information must have been provided by the first disclosure.

8.4 Privacy and fair processing notices

8.4.1 The Company uses privacy notices to convey the information listed in the sections above at the point of data collection.

8.5 The purpose changes

8.5.1 If the original purpose for which the data that was collected changes, then the data

subject must be informed of the new purpose. They must also be informed of any changes to the information already provided under the points in this section.

8.6 Multiple controllers

8.6.1 In a situation where the Company should act jointly with other organisations as a controller, then respective responsibilities will be clearly laid out between the parties.

9 PRIVACY BY DESIGN AND BY DEFAULT

9.1 The Company embeds data protection into the design of every system that uses personal data, so that it is protected throughout its entire lifecycle. To maintain this principle, all members of staff are required to:

9.1.1 Ensure personal data is mapped, classified into either personal or special category data, labelled, stored and accessible so that it is easily found if need be (eg in the event of a subject access request, the need to remove the data or the need to update the data).

9.1.2 Ensure our systems continue to function so that any personal data that is added may be deleted automatically (where appropriate).

9.1.3 Ensure that any new documentation which collects personal data is drafted in such a way that no personal data is requested in excess of what is necessary to achieve the purpose.

9.1.4 Ensure that a data subject is only identified for as long as necessary. This may include removing an identifier such as a name or date of birth.

Ensure that any new system will process data in a format that is commonly used.

10 DATA PROTECTION IMPACT ASSESSMENTS

A Data Protection Impact Assessment (DPIA) has been carried out in respect of processing that is considered likely to put the rights and freedoms of data subjects at a high risk.
A Data Protection Impact Assessment must always be completed if the processing of personal data is likely to be high in risk to the rights and freedoms of the data subject. Examples of processing that may be high risk include; systematic monitoring of publicly accessible information on a large scale, or profiling that may significantly affect individuals.

11 INFORMATION SECURITY

As a company we regularly review our approach to information security and stay up to date with developments in the field and emerging threats. To secure the information we hold we are committed to allocating sufficient resources (including time and budget) to ensure that robust and high-quality tools and processes are implemented.
The Company takes all reasonable steps to protect and maintain the integrity, confidentiality and availability of personal data. For the purposes of this policy, organisational and technological security measures are in place to protect and secure against: accidental loss, damage, destruction, theft or unsanctioned disclosure, publication or transfer of personal data.

11.1 Protection: All members of staff and any associated third parties are made aware of their responsibilities and are required to exercise and uphold every applicable security measure.

11.2 Integrity: All members of staff and any associated third parties are made aware of their responsibilities and are required to securely update and maintain completeness of personal data.

11.3 Confidentiality: All members of staff and any associated third parties are made aware of their responsibilities and are required to only access personal data which they are authorised to process. Those with authority to process personal data will only make personal data available to recipients (other colleagues, third parties etc) if those recipients are authorised to access or process the data.

11.4 Availability: The Company has taken measures to prevent accidental and deliberate unauthorised access. This includes disaster recovery and business continuity arrangements. All members of staff, agency workers and any associated third parties are made aware of their responsibilities and are required to maintain the measures put in place by the Company to physically and virtually secure information. If they detect any threats to the continued availability of access to assets, systems and information they must report this to a line manager so that it may be escalated appropriately. Threats may include: damage to a computer or filing system, faulty locks, viruses or malware.

11.5 This section is applicable to self-employed persons and contractors in so far as they will be asked to ensure compliance with these points and our security measures. In any event, they will be required to uphold obligations under applicable data protection laws at all times and without exception. Failure to do so will enable the Company to terminate the service agreement without notice and the incident may be reported to the relevant supervisory authority.

12 TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

12.1 There my be exceptional circumstances where we transfer personal data outside of the European Economic Area ("EEA"), we have ensured that the following condition(s) apply:

- The EU Commission has determined that the country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The Company has appropriate safeguards which support the rights of data subjects. These include asking direct permission from the subjects before any data is transferred out of the Company or outside of the EEA.

13 RECORD KEEPING

The Company maintains records of data processing activities in accordance with data protection legislation. Record keeping is carried out for the following processing activities:

- Processing of personal data which is likely to result in a risk to the rights and freedoms of data subjects
- Processing of personal data which is regular and frequent
- Processing of personal data which includes special category data
- Processing of personal data which includes data about criminal convictions

14 BREACH AND INCIDENT REPORTING

14.1 Serious breaches must be reported to the relevant supervisory authority within 72 hours of becoming aware of the breach. Therefore, all employees and workers must immediately report an incident that may potentially or actually put personal data at risk of a data breach. This is never more imperative than when it is suspected that there may be actual loss, theft unauthorised disclosure or inappropriate use of personal data, either wholly or partly. In this event you must immediately refer to and follow the Company's Breach and Incident and Reporting Procedure.

14.2 Where a third-party service provider notifies you of an incident that may affect the Company and its responsibilities, you must immediately report the incident. In this event you must immediately refer to and follow the Company's Breach and Incident Reporting Procedure.

15 THE RIGHTS OF DATA SUBJECTS

The Company shall be diligent in providing data subjects information about their rights and in complying with any appropriate assertions of their rights.

15.1.1 All reasonable efforts will be made to verify the identity of the data subject before carrying out any requests or disclosures of information made by them. These efforts may include the request for additional personal information if necessary.

15.1.2 The following rights apply to all data subjects:

- Right of transparent communication
- Right of access
- Right to rectification
- Right to erasure (right to be forgotten)
- Right to restriction of processing
- Obligation to notify recipients
- Right to data portability
- Right to object
- Right to not be subject to automatic decision making

16 SUBJECT ACCESS REQUESTS

16.1 Making a request

16.1.1 If you wish to make a subject access request to verify the lawfulness and accuracy of the personal data we hold about you, then you are encouraged to put your request in writing (letter or e-mail) and submit it to the Registered Data Controller Email: Ronnie@careerstudio.co.uk.

16.1.2 Your request should be specific about the nature and the type of data you require.

16.1.3 Every attempt will be made to comply with your request in a timely manner and without undue delay.

16.1.4 Upon receipt of the information you are encouraged to check the accuracy of the information and to advise the Company of any updates that may need to be made.

16.1.5 A fee will not be charged for an access request, except where a request is deemed to be 'manifestly excessive' or you have already been provided with the information.

16.2 Receiving a request

16.2.1 If you receive a request, you should pass it to the Registered Data Controller immediately.

16.2.2 Requests must be acknowledged upon receipt.

16.2.3 Requests must be complied with in a timely manner and without undue delay. If it is anticipated that compliance with a request is not going to be immediate then the Controller should be notified and informed of the legitimate reasons for this. The information requested must be provided within one month of receipt of the request.

16.2.4 If an extension to the time line is absolutely necessary under exceptional circumstances, then any extension must be agreed by the data subject and signed off by the Controller within one month of the request. If an extension is agreed, then the information must be provided within a maximum of three months from the receipt of the request.

16.2.5 If a request is received electronically (eg via e-mail) then the request must be responded to electronically.

16.2.6 The data must be provided in a common format (eg a paper file, a pdf document etc.).

16.2.7 Only personal data pertaining to the individual who made the request should be released.

16.2.8 If there is any doubt over the identity of the individual making the access request, then reasonable steps must be taken to verify their identity, before complying with the request.

16.2.9 When the personal data is provided, the individual must be informed of the right to lodge a complaint with the relevant supervisory authority and the existence of the right to objection, rectification, erasure and restriction of the data.

16.2.10 The data subject may be directed to the relevant privacy/fair processing notice which will provide advice on the conditions for processing.

17 GENERAL GUIDANCE FOR EMPLOYEES

17.1 We recognise that there are different areas in the organisation where members of staff may be responsible for processing personal data in different ways. We also recognise that responsibilities and nuances in processing are likely to vary across specialisms and levels of seniority.

17.2 The Company will provide guidance to staff when processing personal data specific to their job. This information shall include:

- A description of the limitations which surround how personal data can be used.
- The steps that must be followed to ensure that personal data is maintained accurately.
- A comprehensive discussion of security obligations, including all reasonable steps that should be taken as a minimum to prevent unauthorised access or loss.
- Confirmation of whether the transfer of personal data shall be permitted. Transfer of personal data is prohibited unless specific legitimate grounds have been established.
- Specific information regarding the way in which personal data should be handled when it is destroyed or deleted.

18 General responsibilities of management

18.1 All members of the senior management are responsible for championing and enforcing this policy to all other staff within the Company, whenever appropriate.

18.2 Particular roles within senior management are responsible for assessing the business risk arising as a result of processing personal data. These roles include all Directors, Managers and Executives.

18.3 Those members of senior management identified above are required to work with the Company to develop procedures and controls to identify and address risks appropriately.

18.4 Responsibility will be allocated to individual roles for determining risk-based technical, physical and administrative safeguards including safeguards for equipment, facilities and locations where personal data is stored; establishing procedures and requirements for collecting, transporting, processing, storing, transferring (where appropriate) and destroying personal data. These considerations must also be given when dealing with any third parties who may be authorised or obligated to process personal data on behalf of the Company.

19 NON-COMPLIANCE

19.1 This policy along with associated documents, seeks to guide and instruct all member of staff on how they ensure compliance with data protection laws to which the Company is subject.

19.2 If a member of staff should fail to comply with applicable data protection laws, they may subject the Company and themselves as individuals to civil and criminal penalties. This is likely to jeopardise the reputation of the Company and as a result may impact on the operational and performance capabilities of the business.

19.3 As the ramifications of non-compliance are potentially severe, any failure to comply with this policy or reasonable instruction given in connection with the protection and security of personal data, may result in disciplinary action. Serious, deliberate or negligent transgressions may be regarded as gross misconduct and if substantiated, may result in summary dismissal (without notice).

19.4 Third parties, contractors and self-employed persons

19.4.1 If any self-employed person, contractor or third party is found to be failing to meet obligations with applicable data protection laws then notice may be served on the contract for service.

19.4.2 Serious, deliberate or negligent transgressions may permit the Company to terminate the contract for service with immediate effect. In this event, all reasonable steps will be taken to recover and protect the personal data concerned and the relevant supervisory authority will be notified. Where the rights and freedoms of data subjects are likely to be at risk, the data subjects will be notified without delay.

20 RELATED POLICIES AND DOCUMENTS

- Career Studio (Scotland) Ltd Policy Handbook

21 FURTHER INFORMATION

Any queries or comments about this policy, or any concerns that the policy has not been followed, should be addressed to Ronnie Davidson, Career Development Director Email: ronnie@careerstudio.co.uk. Career Studio (Scotland) Ltd, Granary Business Centre, Coal Road, Cupar, Fife KY15 5YQ.

22 POLICY OWNER

This policy is owned and maintained by Ronnie Davidson, Career Development Director.

23 POLICY REVIEW DATE

Date last reviewed: 5th June 2019