Data Protection Policy

Appendix 7

CareersInc Ltd (the Company) collects and uses certain types of personal information about contracted workers, students, parents and other individuals who come into contact with the Company. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the General Data Protection Regulation (GDPR) and other related legislation.

1 Personal Data

'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain. A subset of personal data is known as 'special category personal data'. This special category data is information that relates to:

1.1.1. race or ethnic origin;

1.1.2. political opinions;

1.1.3. religious or philosophical beliefs;

1.1.4. trade union membership;

1.1.5. physical or mental health;

1.1.6. an individual's sex life or sexual orientation;

1.1.7. generic or biometric data for the purpose of uniquely identifying a natural person

1.2. Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.

1.3. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

1.4. The Company does not intend to seek or hold sensitive personal data about any students/ parents or clients who access it's service. All data about students will be accessed, as necessary, via school IT systems and will not be held on any Company IT equipment. The Company does not intend to seek or hold sensitive personal

data about contracted workers except where the Company has been notified of the information, or it comes to the Company's attention via legitimate means (e.g. a disclosure) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Contracted workers are under no obligation to disclose to the Company their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and / or parenthood are needed for other purposes, e.g. pension entitlements).

1.5. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

1.6. Anybody who makes a request to see any personal information held about them by the Company is making a subject access request. All information relating to the individual, including that held in electronic or manual files.

2 The Data Protection Principles

2.1 The six data protection principles as laid down in the GDPR are followed at all times:

- Personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;
- Personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;
- personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;
- personal data shall be accurate and, where necessary, kept up to date;
- personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose / those purposes;
- personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.
- In addition to this, the Company is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law
- The Company is committed to complying with the principles in 2.1 at all times. This means that the Company will:

- inform individuals as to the purpose of collecting any information from them, as and when we ask for it;
- be responsible for checking the quality and accuracy of the information;

- regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the data retention policy;
- ensure that when information is authorised for disposal it is done appropriately;
- ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system
- share personal information with others only when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests for access to personal information known as subject access requests and report any breaches of the GDPR

3 Conditions for processing in the first data protection principle

3.1 The individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given.

3.2 The processing is necessary for the performance of a contract, to which the individual is a party, or is necessary for the purpose of taking steps with regards to entering into a contract with the individual, at their request.

3.3 The processing is necessary for the performance of a legal obligation to which we are subject.

3.4 The processing is necessary to protect the vital interests of the individual or another.

3.5 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 us.

3.6 The processing is necessary for a legitimate interest of the Company or that of a third party, except where this interest is overridden by the rights and freedoms of the individual concerned.

4 Contracted workers/ Customer and stakeholder data

4.1 The personal data held about contracted workers will include contact details, employment history, information relating to career progression, information relating to DBS checks and professional qualifications.

4.2 The data is used to comply with legal obligations placed on the Company in relation to contracting with professionally qualified workers who meet DBS clearance standards in relation to the education of children in a school environment. The Company may pass information to other regulatory authorities where appropriate, and may use names and

photographs of workers in publicity and promotional material. Personal data will also be used when giving references.

4.3 The Company will hold Customer contact and stakeholder contact details in order to offer contracted careers guidance services. This will include contact details of school staff and employers and providers who may support events and activities organised for students and parents/carers.

5 Security of personal data

5.1 The Company will take reasonable steps to ensure that only Directors have access to personal data relating to workers in order to meet business needs and for the recruitment and retention of workers. All workers will be made aware of this Policy and their duties under the GDPR. The Company will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

5.2 The Company will take reasonable steps to ensure that only Directors and contracted workers have access to personal data relating to Customers and stakeholders outlined in 4.3.

6 Disclosure of personal data to third parties

6.1The following list includes the most usual reasons that the Company will authorise disclosure of personal data to a third party:

- To give a confidential reference relating to a current or former contracted worker
- For the prevention or detection of crime;
- For the assessment of any tax or duty;
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon the Company (other than an obligation imposed by contract);
- For the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- For the purpose of obtaining legal advice;
- For research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);

All requests for the disclosure of personal data must be sent to the Company Directors, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

7 Other rights of individuals

The Company has an obligation to comply with the rights of individuals under the law, and takes these rights seriously. The following section sets out how the Company will comply with the rights to:

- object to processing;
- rectification;
- erasure; and
- data portability

Right to object to processing

An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest where they do not believe that those grounds are made out.

Where there is an objection this must be made in writing to the Company Directors, who will assess whether there are compelling legitimate grounds to continue processing which overrides the interests, rights and freedoms of individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

Right to rectification

An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the Company Directors and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data, and communicated to the individual. The individual shall be given the option of [a review under the data protection complaints procedure, or] an appeal direct to the Information Commissioner.

An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

- Where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
- Where consent is withdrawn and there is no other legal basis for the processing;
- an objection has been raised under the right to object, and found to be legitimate;
- personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

- Where there is a legal obligation on the Company to delete.

Company Directors will make a decision regarding any application for erasure of personal data, and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other data controllers, and / or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

In the following circumstances, processing of an individual's personal data may be restricted:

- Where the accuracy of data has been contested, during the period when the Company is attempting to verify the accuracy of the data;
- Where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
- Where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

8 Breach of any requirement of the GDPR

If there has been an objection made about the personal data held as outlined above, the following process will be used: pending the outcome of any decision.

Once notified, the Company Directors will assess:

- The extent of the breach;
- The risks to the data subjects as a consequence of the breach;
- Any security measures in place that will protect the information;
- Any measures that can be taken immediately to mitigate the risk to the individuals.

Unless the Company Directors conclude that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Company, unless a delay can be justified.

The Information Commissioner shall be told:

- Details of the breach, including the volume of data at risk, and the number and categories of data subjects;
- The contact point for any enquiries
- The likely consequences of the breach;
- Measures proposed or already taken to address the breach.
- If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then a Company Director shall notify data subjects of the breach without

undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals.

Data subjects shall be told:

- The nature of the breach;
- Who to contact with any questions
- Measures taken to mitigate any risks
- A Company Director shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed and a decision made about implementation of those recommendations.

Privacy Notice for Contracted Workers

Who we are

As you are aware you have a contract with CareersInc Ltd and for the purposes of Data Protection legislation, the Company Directors act as the Data Controllers. This means they will access personal data about you.

The postal address of the Company is: 4 Atlas, First Point, Doncaster DN4 5JT

The Company Directors can be contacted on:
Jacqui.jameson@careersinc.uk and deb.norton@careersinc.uk

In this policy 'we' and 'us' means the Company.

How we use your information

We process personal data relating to those we contract with to support the delivery of independent and impartial information, advice and guidance services. This is for contracting purposes to assist in the running of the Company and / or to enable individuals to be paid.

This personal data includes identifiers such as names, contract details, remuneration details, qualifications and bank details. We hold a copy of a CV for each contracted worker as well as their Disclosure and Barring Service (DBS) registration number and date of issue.

During the recruitment process we may receive information about you from a previous employer or an educational establishment which you have previously attended. You will know about this because you will have supplied us with the relevant contact details.

Collecting and using your information in this way is lawful because:

- The processing is necessary for the performance of your contract
- The processing is necessary for the performance of a legal obligation to which the Company is subject, for example our legal duty to safeguard pupils in the schools we work in
- The processing is necessary to protect the vital interests of others, i.e. to protect pupils from harm

How we share your information with third parties

We will share your DBS registration number and date of issue with the schools you are working in but will not share other information about you with third parties without your consent unless the law allows us to.
We will share your identity and pay information with HMRC in conjunction with your legal obligation to pay income tax and make national insurance contributions if this is requested.

Our disclosures to third parties are lawful because one of the following reasons applies:

- The disclosure is necessary for the performance of your contract
- The disclosure is necessary for the performance of a legal obligation to which the Company is subject, for example our legal duty to safeguard pupils in the schools we work in.
- The disclosure is necessary to protect the vital interests of others, i.e. to protect pupils from harm

How long we keep your personal information

We only keep your information for as long as we need it or for as long as we are required by law to keep it. Full details are given in our Records Retention Policy which can be found in the Company's HR Handbook or can be requested from a Company Director.

Your rights

You have the right to:

- Ask for access to your personal information
- Ask for rectification of the information we hold about you
- Ask for the erasure of information about you
- Ask for our processing of your personal information to be restricted
- Data portability
- Object to us processing your information.

If you want to use your rights, for example, by requesting a copy of the information which we hold about you, please contact a Company Director.

More information about your rights is available in our Data Protection Policy in the HR Handbook for Contracted Workers.

If at any time you are not happy with how we are processing your personal information, then you may raise the issue with a Company Director and if you are not happy with the outcome you may raise a complaint with the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow

CareersInc Ltd updated in September 2018

Cheshire
SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 if you prefer to use a national rate number

Contractor Personal Data

I understand that CareersInc Ltd will hold the following personal data in order to meet the contractual requirements of the organisations they support:

- My CV
- Confirmation that a CareersInc Director has seen original certificates of training and qualifications required by the company to prove I am competent and qualified to undertake any contracted work offered by the company.
- MY DBS certificate number and date of issue, which they will share with academies and MATs I may be contracted to work in. I agree to show my original DBS clearance certificate to nominated staff in academies attended on my first day of work there.
- Payroll/ bank information so that monthly payments can be made to me
- Observations of Professional Practice feedback
- CDI membership number
- A signed copy of my contract with CareersInc Ltd

I confirm that I understand and agree that CareersInc will keep the details above, and for up to 24 months after my contract with them terminates, so that they can provide any references etc for me.

Details of the above will be stored on password secured computers and accessible only by Company Directors. In addition, a paper copy of your CV will be stored securely and also only accessible by Company Directors.

I understand that I can access the personal details held by requesting this in writing to a CareersInc Director, who will provide access within 30 working days.

Paper records will be shredded with immediate effect.

Print Name:	Date:
Signed:	

Guidance for Staff on How to Protect Data and ensure compliance with Data Protection Legislation and GDPR.

Below is some practical guidance and steps you can take to protect the data that you currently hold or have access to. This will hopefully protect you, the Company and the Data Subjects.

1. Don't store personal data on memory sticks (USB)

A memory stick has a greater risk of being lost, or may not have appropriate encryption on it.

2. If you use your own devices to access academy data, it must be secure

If you use your own personal phone, tablet or computer to access your email, you must ensure that it is adequately encrypted and password protected. **Never save any individual student data on your CareersInc ipad or your own devices.**

3. Ensure all requests for data are in writing

If you receive a request for personal data from the Police, Social Care, or other body that has a legitimate reason for requesting it, you must refer the request to the relevant academy.

4. Send personal data securely

If you send information or emails about students to academy staff this must be done on academy password protected IT equipment and **never** via a CareersInc email. You must ensure that you do not forward communication about students via an academy email to a CareersInc email at a later date as student details may get "tagged" on from earlier correspondence.

5. Lock your screen when you leave

Every time you leave your laptop or computer you MUST ensure that the screen is locked. Failure to do this could provide access to the MIS or other sensitive information saved on the network for students or other people within the academy who do not have the right to see this data.

6 **Always clean your desk and lock any windows when you finish your work in an academy.**

If you have a hard copy of notes they must be locked away securely, and you should make sure that they do not hold full names of students or anything that would identify them to others. Try to minimise the risk by using initials or first names only rather than full names.

7. Check, check and check again

If you are sending written information about students e.g. Summaries of Guidance to other staff in the academy, please ensure:

- The name and address are correct;
- That nothing has been accidently attached to the letter/document;
- That the name on the letter/document matches the address on the envelope.
- Where you have photocopied, or printed information please make sure you remove all copies from printers etc.

Ideally, academy staff will be responsible for distribution of written information.

8.

Never collect images/ photos/ videos of students on company or personal equipment. If you are running events in schools and want to collect images for evaluation or publicity purposes, please ensure that this is done on academy equipment and you have the permission of a member of SLT in that academy.

9. Report any loss of data

If you think data has been lost or stolen, report it immediately to the relevant academy and a CareersInc Director.

CAREERSINC

Retention Policy and Destruction of Data

Type of Record / Document	**Retention Period**
Data Protection and Safeguarding Policies and procedures	Retain as part of HR Handbook for contracted workers and updated in line with legislation.
Accounting Records Accounting records Tax returns VAT returns	Minimum 6 years
Contracts and agreements	Minimum of 6 years from completion of contractual obligations or term of agreement, whichever is the later
IP/ IT agreements (including software licences and ancillary agreements eg maintenance etc)	Minimum of 6 years from completion of contractual obligations or term of agreement, whichever is the later
Contracted workers records CVs for all workers	Stored securely and electronically for length of contract period and for up to 2 years after a contract ends. Accessible only by Company Directors
DSB checks	Retain details of DBS registration number and date of issue for all contracted workers during contract period. Retain these details for up to 2 years after any contracted workers cease contracts with the Company
Contracts for services	Annual contracts issued to each contracted worker. Retained for 12 months during contracted period and updated annually if contractor retained.
Bank details for contracted workers	Retained for contract period
CVs from speculative applicants	

	Retained securely and electronically for up to 2 years and accessible only by Company Directors Updated permissions every two years
Insurance Records Insurance policies for public and professional indemnity Correspondence related to claims	Duration of policy (or as required by policy) Minimum 7 years
Provider/ employer data base who might support career events	Stored electronically and accessible by careers advisers. Updated permissions every two years.

Destruction of hard copy data

Paper records will be shredded as appropriate.