1. Data Protection Policies RG11

Data Protection Policy

The security and privacy of your data is taken seriously by us, but we need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We are committed to complying with all the legal obligations surrounding Data Protection.

This policy applies to current and former employees, workers, volunteers, interns, apprentices and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

The Company has separate policies and privacy notices in place in respect of other categories of data subject. A copy of these can be obtained from the person responsible for Data in the Company.

The Company has taken steps to protect the security of your data in accordance with our Data Security Policy and will train staff about their data protection responsibilities as part of the induction process. We will only hold data for as long as necessary for the purposes for which we collected it.

The Company is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, the Company.

This policy does not form part of your contract of employment (or contract for services if relevant) and can be amended by the Company at any time.

Data Protection Principles

Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- Be processed fairly, lawfully and transparently;
- Be collected and processed only for specified, explicit and legitimate purposes;
- Be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- Be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
- Not be kept for longer than is necessary for the purposes for which it is processed; and
- Be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

How we define personal data

'**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by you, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. It could be provided or created during the recruitment process or during the course of the contract of employment (or services) or after its termination. It could be created by your manager or other colleagues.

The types of personal data we collect and use about you is included in the Privacy Notice that is issued with your contract of employment.

How we define special categories of personal data

'**Special categories of personal data**' are types of personal data consisting of information as to:

- Your racial or ethnic origin;
- Your political opinions;
- Your religious or philosophical beliefs;
- Your trade union membership;
- Your genetic or biometric data;
- Your health;
- Your sex life and sexual orientation; and
- Any criminal convictions and offences.

We may hold and use any of these special categories of your personal data, as detailed in the Privacy Notice, in accordance with the law.

How we define processing

'**Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

How will we process your personal data

The Company will process your personal data (including special categories of personal data). We will use your personal data for:

- performing the contract of employment (or services) between us;
- complying with any legal obligation; or
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs). You have the right to challenge our legitimate interests and request that we stop this processing.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

Examples of when we might process your personal data can be found in the Privacy Notice. We will only process special categories of your personal data in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the person for responsible for Data in the Company.

We do not need your consent to process **special categories** of your personal data when we are processing it for the following purposes, which we may do:

- Where it is necessary for carrying out rights and obligations under employment law;
- Where it is necessary for carrying out rights and obligations under legislation governing the provision of children's services (including processing your criminal record data);
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent;
- where you have made the data public;
- where processing is necessary for the establishment, exercise or defence of legal claims; and

- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

We might process special categories of your personal data for the purposes stated in the Privacy Notice, in particular, we may use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety; and
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.
- your criminal record including details of convictions and offences to ascertain your initial and ongoing suitability for employment, meet our legal obligations and safeguard young people.

We do not take automated decisions about you using your personal data or use profiling in relation to you.

Sharing your personal data

Sometimes we might share your personal data with group companies or our business partners, contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

We use the following contractors to carry out our Company business:

- Vetting check provider to process DBS checks
- Legal advisers

We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

How should you process personal data for the Company

Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's IT Security and Data Retention policies.

The Company's Data Protection Officer is responsible for reviewing this policy on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person and address any written requests to them.

You should only access personal data covered by this policy if you need it for the work you do for, or on behalf of the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

- You should not share personal data informally.
- You should keep personal data secure and not share it with unauthorised people.
- You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.
- You should not print or make unnecessary copies of personal data and should keep and dispose of any hard copies securely.
- You should use the passwords set by the IT department on all hardware and not change these without prior authorisation.
- You should lock your computer screens when not at your desk or when leaving your laptop unattended.
- Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

- Do not access or save personal data on your own personal computers or other devices including phones, USB drives, disks and memory cards.
- Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the person for responsible for Data in your Company.
- You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.
- You should not take personal data away from Company's premises without authorisation from your line manager or from the person for responsible for Data in your Company.
- Personal data should be shredded and disposed of securely when you have finished with it.
- You should ask for help from the person for responsible for Data in your Company if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
- Any deliberate or negligent breach of this policy by you will be investigated and may result in disciplinary action being taken against you in accordance with our disciplinary procedure.
- It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

How to deal with data breaches

We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner's Office within 72 hours.

If you are aware of a data breach you must contact of the person for responsible for Data immediately and keep any evidence you have in relation to the breach.

Subject Access request

Data subjects can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request, you should forward it immediately the person for responsible for Data in your Company who will coordinate a response.

If you would like to make a SAR in relation to your own personal data, you should make this in writing to the person for responsible for Data in the Company. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

Your data subject rights

- You have the right to information about what personal data we process, how and on what basis as set out in this policy.
- You have the right to access your own personal data by way of a subject access request (see above).
- You can correct any inaccuracies in your personal data. To do you should contact of the person for responsible for Data in the Company.
- You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact the person for responsible for Data in the Company.
- While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact the person for responsible for Data in the Company.
- You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
- You have the right to object if we process your personal data for the purposes of direct marketing.

- You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.
- With some exceptions, you have the right not to be subjected to automated decision-making.
- You have the right to be notified of a data security breach concerning your personal data.
- In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact the person for responsible for Data in the Company.
- You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.

Data Breach Notification Procedure

1. Purpose

Care Today Children' Services and Parallel Parents Ltd ("we"/"us") have this procedure in place to provide a standardised response to any reported data breach incident and ensure that data breaches are appropriately logged and managed in accordance with the law and best practice.

2. Scope

This procedure applies in the event of a personal data breach and applies to all employees of Care Today Children' Services and Parallel Parents Ltd at all times and whether located within the physical offices or not.

The document applies to all information we hold, and all information technology systems utilised by us.

3. Responsibility

3.1 All employees/staff, contractors or temporary employees/staff and third parties working for or on behalf of us are required to be aware of, and to follow this procedure in the event of a personal data breach.
3.2 All employees/staff, contractors or temporary personnel are responsible for reporting any personal data breach to the Data Protection Officer who's contact details are as follows:
Name: Patrick Thomas / Samantha Bradwell
Telephone: 0161 477 5830
Email: admin@caretoday.co.uk

4. Definition

The GDPR defines a "personal data breach" in Article 4(12) as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Examples include:

- Loss or theft of data or equipment on which data is stored
- Access to data by an unauthorised third party
- Sending personal data to an incorrect recipient, whether via post, fax or email
- Alteration of personal data without permission
- Loss of availability of personal data such as equipment failure
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceit.

For the purposes of this procedure data security breaches include both confirmed and suspected incidents.
If you suspect a data breach or are unsure whether the incident which has occurred constitutes a data breach please refer the matter to the Data Protection Officer for consideration

5. Reporting an incident

5.1 Any individual who accesses, uses or manages information within our business is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer.
5.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.
5.3 The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, the nature of the information, and how many individuals are involved.

6. Next Steps

6.1 The Data Protection Officer will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.
6.2 An initial assessment will be made by the Data Protection Officer in liaison with relevant persons (which may include IT services) to establish the severity of the breach and who will take the lead investigating the breach (this will depend on the nature of the breach).
6.3 An investigation will be undertaken immediately and wherever possible within 24 hours of the breach being discovered/reported.
6.4 The Data Protection Officer will investigate the risks associated with the breach, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.
6.5 The Data Protection Officer will then establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.
6.6 The Data Protection Officer will identify who may need to be notified. The relevant procedures from those identified below will then be followed. Every incident will be assessed on a case by case basis.

7. Procedure – Breach notification data controller to supervisory authority

7.1 The Data Protection Officer will determine if the supervisory authority (the Information Commissioner's Office (ICO) in the UK) need to be notified in the event of a breach.
7.2 If the breach affects individuals in different EU countries, the ICO may not be the lead supervisory authority. The Data Protection Officer will also need to establish which European data protection agency would be the lead supervisory authority for the processing activities that have been subject to the breach.
7.3 We will assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach, by conducting an investigation and/or an impact assessment. If we decide that we do not need to report the breach to the ICO we will justify and document our decision.
7.4 If a risk to data subject(s) is likely, the Data Protection Officer will report the personal data breach to the ICO without undue delay, and not later than 72 hours after becoming aware of it.
7.5 If the data breach notification to the ICO is not made within 72 hours, Data Protection Officer will submit notification electronically with a justification for the delay.
7.6 If it is not possible to provide all of the necessary information at the same time we will provide the information in phases without undue further delay.
7.7 The following information needs to be provided to the supervisory authority:

- 7.7.1 A description of the nature of the breach.
- 7.7.2 The categories of personal data affected.
- 7.7.3 Name and contact details of the Data Protection Officer.
- 7.7.4 Likely consequences of the breach.
- 7.7.5 Any measures taken to address the breach.
- 7.7.6 Any information relating to the data breach.
- 7.7.7 Approximate number of data subjects affected.
- 7.7.8 Approximate number of personal data records affected.

7.8 The breach notification should be made via telephone - **ICO: 0303 123 1113.** Alternatively, if the Data Protection Officer may choose to report it online if they are still investigating and will be able to provide more information at a later date or if they are confident that the breach has been dealt with appropriately.
7.9 In the event the ICO assigns a specific contact in relation to a breach, these details are recorded in the Internal Breach Register

8. Procedure – Breach notification data controller to data subject

8.1 If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Care Today Children' Services and Parallel Parents Ltd will notify those/the data subjects affected without undue delay and in accordance with the Data Protection Officer recommendation.
8.2 A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. In any event the Data Protection Officer will document their decision-making process.
8.3 We will describe the breach in clear and plain language, in addition to information specified in clauses 7.7.1-7.7.6 above.

8.4 The data controller takes subsequent measures to ensure that any risks to the rights and freedoms of the data subjects are no longer likely to occur.
8.5 If the breach affects a high volume of data subjects and personal data records, we will make a decision based on assessment of the amount of effort involved in notifying each data subject individually, and whether it will hinder our ability to appropriately provide the notification within the specified time frame. In such a scenario a public communication or similar measure informs those affected in an equally effective manner and will be considered by the Data Protection Officer, who's decision will be final.
8.6 If we have not notified the data subject(s), and the supervisory authority considers the likelihood of a data breach will result in high risk, Organisation Name will communicate the data breach to the data subject by telephone or email.
8.7 We will document any personal data breach(es) within the Data Breach Register, incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

9. Documentation requirements

Internal breach register: there is an obligation for us to document each incident "comprising the facts relating to the personal data breach, its effects and the remedial action taken".

10. Evaluation

10.1 Once the initial incident is contained, the Data Protection Officer will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken.
10.2 Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.
10.3 The review will consider various points, including but not limited to:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary Identifying weak points within existing security measures
- Staff awareness

Employee Privacy Notice

Care Today Children' Services and Parallel Parents Ltd are committed to protecting the privacy and security of your personal information and we will always treat you and your data with the respect you deserve.

This Privacy Notice covers how we collect, use, store and disclose the data that you supply to us and your rights about data that we hold about you. It applies to current and former employees, workers, volunteers, interns and contractors and does not form part of any contract of employment or other contract to provide services. For more information please contact the Data Protection Officer (Kieran Touhey) who will provide you with our data protection policy.

THE INFORMATION WE COLLECT FROM YOU

Personal individual information means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). We will collect, store, and use the following categories of personal information about you:

1. Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
2. Date of birth.
3. Gender.
4. Marital status and dependants.
5. Next of kin and emergency contact information.
6. National Insurance number.
7. Bank account details, payroll records, travel logs and expenses and tax status information.
8. Salary, annual leave, pension and benefits information.
9. Start date.
10. Location of employment or workplace.
11. Access to your DVLA portal.
12. Recruitment information (including copies of right to work documentation, passport, references and other information included in a CV or cover letter or as part of the application process).
13. Employment records (including job titles, work history, working hours, training records and professional memberships).
14. Compensation history.
15. Performance information.
16. Disciplinary and grievance information.
17. CCTV footage and other information obtained through electronic means such as swipecard records.
18. Information about your use of our information and communications systems.
19. Photographs.

We may also collect, store and use "special categories" of more sensitive personal data which require a higher level of protection:

20. Information about your health, including any medical condition, health and sickness records (including Occupational Health records).
21. Absence notes
22. Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions.
23. Trade union membership.
24. Genetic information and biometric data.
25. Information about criminal convictions and offences.

How the information is collected

We collect personal information through the application and recruitment process, either directly from candidates or sometimes from an employment agency. We may sometimes collect additional information from third parties including former employers or other background and vetting check companies. We may

collect additional personal information in the course of job-related activities throughout the period of you working for us.

When we will use your personal information

We need all the categories of information identified above primarily to allow us to perform our contract with you[*] and to enable us to comply with legal obligations[**]. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties[***] (provided your interests and fundamental rights do not override those interests). We will process your personal information as follows, the asterisks show the purpose for processing:

Purpose	Type of data	Lawful basis
Making a decision about your recruitment or appointment.	1, 12, 13, 25	***
Determining the terms on which you work for us.	8, 9, 10, 12, 13	***
Checking you are legally entitled to work in the UK.	1, 2, 6, 11	**
Paying you and, if you are an employee, deducting tax and National Insurance contributions.	1, 6, 7, 8	** *
Liaising with your pension provider.	1, 2, 6, 8, 9	*
Administering the contract we have entered into with you.	1, 5, 6, 7, 8, 9, 10, 15, 16, 22	*** *
Business management and planning, including accounting and auditing.	1, 2, 3, 6, 7, 8, 9, 10, 15, 16, 18, 20, 22, 23	***
Conducting performance reviews, managing performance and determining performance requirements.	1, 8, 9, 10, 15, 16, 17, 18, 22	*** *
Making decisions about salary reviews and compensation.	1, 7, 8, 9, 10, 12, 13, 15, 16, 17, 18	*** *
Assessing qualifications for a particular job or task, including decisions about promotions.	1, 12, 13, 15, 16, 22	*** *
Gathering evidence for possible grievance or disciplinary hearings.	1, 15, 16, 17, 18, 22	*** *
Making decisions about your continued employment or engagement.	1, 15, 16, 17, 18, 22, 25	*** *
Making arrangements for the termination of our working relationship.	1, 6, 7, 8, 15, 16, 22	*** *
Education, training and development requirements.	1, 13, 15, 16, 22	*** *

Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.	1, 7, 8, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24	***
Ascertaining your fitness to work and managing sickness absence.	1, 2, 3, 4, 5, 10, 15,16, 17, 18, 19, 20, 22	*** *
Complying with health and safety obligations.	1, 5, 10, 22	** *
To prevent fraud.	1, 6, 7, 11, 12, 13, 24, 25	***
To monitor your use of our information and communication systems to ensure compliance with our IT policies.	1, 17, 18	***
To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.	1, 17, 18	***
To conduct data analytics studies to review and better understand employee retention and attrition rates.	1, 2, 3, 4, 20, 22	***
Equal opportunities monitoring.	1, 2, 3, 4, 20, 22	***

Please refer to our Data Protection Policy on the intranet which provides more detail on how we collect your data, the basis on which we hold it and how we store, use and destroy it.

Failure to provide information

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing employee benefits), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

SENSITIVE PERSONAL INFORMATION

"Special categories" of particularly sensitive personal information require higher levels of protection. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations and in line with our Data Protection Policy.
3. Where it is needed in the public interest, such as for equal opportunities monitoring, and in line with our Data Protection Policy.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such

information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

Our obligations as an employer

We will use your particularly sensitive personal information in the following ways:

- We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
- We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.
- We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.
- Your criminal record including details of convictions and offences to ascertain your initial and ongoing suitability for employment, meet our legal obligations and safeguard young people.

INFORMATION ABOUT CRIMINAL CONVICTIONS

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our relevant policies and procedures.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

We will hold information about your criminal convictions and will access your DBS portal where you have registered for the DBS Update Service.

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. We will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us. We will use information about criminal convictions and offences in the following ways:

- To make decisions on your initial and ongoing suitability for your role
- To ensure the protection and safeguarding of the young people in our care
- To meet our legal obligations for the provisions of children's services

We are allowed to use your personal information in this way to meet our legal obligations and because it is within our legitimate interests to do so.

Your duty to inform us of changes

It is important that the personal information we hold about you is accurate and current, so please let us know if any of your information changes.

DISCLOSURE/DATA SHARING

We may have to share your data with third parties, including third-party service providers (including contractors and designated agents); other entities in the group; in the context of a sale of the business; or with a regulator or to otherwise comply with the law; our insurers and/or professional advisers to manage risks legal disputes. The following activities are carried out by third-party service providers:

- DBS Checks
- Legal advice
- Pension benefit provision

We do this where required by law; where it is necessary to administer the working relationship with you; or where we have another legitimate interest in doing so.

We require third parties to respect the security of your data and to treat it in accordance with the law.

Transfers of data outside of the EU

We will not transfer the personal information we collect about you outside the EU in order to perform our contract with you.

DATA RETENTION

We must store most of your HR data for a period of at least 75 years following the termination of your employment; some personal financial and medical data will be destroyed after 2 years; Health and Safety information must be held for a minimum of 40 years.

YOUR RIGHTS

Your rights in connection with personal information
Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. Please refer to our DSAR Procedure for more information.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.

Right to withdraw consent

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. Please contact the person responsible for Data Protection in our Company.

COMPLAINTS & QUESTIONS

If you have any questions about this privacy notice or how we handle your personal information, please contact the person responsible for Data Protection in our Company. If we have breached our duty of care, we will take appropriate action.

If you are not satisfied by our response you also have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (**Email**: casework@ico.org.uk)

CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Recruitment Privacy Notice

HOW WE USE YOUR DATA FOR RECRUITMENT

Background

This privacy policy covers how Care Today Children's Services / Parallel Parents ltd collect, use, store and protect the data that is supplied to us by job applicants and agencies.

Our Commitment to Job applicants

We believe completely in equal opportunities and will treat all applicants fairly with no discrimination.

We never knowingly provide misleading information about the nature of the role. We would never charge a job seeker a fee for the purpose of finding them a role.

We are committed to managing your personal information securely and with respect in accordance with the General Data Protection requirements.

The information we collect may cover the following:

- Contact information (name address, phone number and email address)
- Information from CV or application form or covering letter (education, skills and qualifications)
- Health records (Night Worker assessment forms, Health questionnaires) where required as part of the role.
- Occupational health report (Higher level screening required for role) with Access to Medical Records consent being given by the applicant
- Disclosure and Barring Record where a requirement for the role
- References from the names referees that the applicant provides and only with the applicants' consent.
- Visa and proof of the right to work in the UK documents
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Salary, annual leave, pension and benefits information.
- Access to your DVLA portal (where driving is required for the role).

We may also collect, store and use "special categories" of more sensitive personal data which require a higher level of protection such as Information about your race or ethnicity, religious beliefs, sexual orientation and political opinions. Also information about criminal convictions and offences.

Purpose of collection

The purpose of collecting this information is to find suitable candidates to fulfil a specific role within our Company, and to check that you are legally entitled to work in the UK. We collect personal information either directly from candidates or sometimes from an employment agency. We may sometimes collect additional information from background check and vetting check providers as well as previous employers.

Where appropriate, we will collect information about criminal convictions as part of the recruitment process. We are allowed to use your personal information in this way to meet our legal obligations and because it is within our legitimate interests to do so.

How the information is held

Most information is transmitted by email and is stored on our computers, and paper-based filing. We use a physical server which is located at our Head Office in Stockport as well as storing some personal data on Google Drive.

All this information can only be accessed by authorised staff within our Company. Our staff are trained to understand the importance of keeping personal data secure.

Our computers are safeguarded by anti-virus software and the regular changing of security passwords.

The information on candidates for specific roles will be held for 6 months in line with CIPD recommended best practice. After which paper files will be securely shredded and computer records deleted. Only if we have asked, and you have given your consent for the data to be held will this not apply.

Disclosure

We may disclose the information for the purpose of obtaining referees. Where additional information is required the information may be disclosed to the Disclosure and Barring Service (or DBS check provider), your G.P or an Occupational Health professional only after you have given your consent

You have specific rights in connection with personal information: request access to your personal information; **request correction** of the personal information that we hold about you; **request erasure** of your personal information; **object to processing** of your personal information where we are relying on a legitimate interest; **request the restriction of processing** of your personal information; **request the transfer** of your personal information to another party and the r**ight to withdraw consent.**

Complaints

Privacy complaints are taken very seriously and if you believe that we have breached your privacy you should in the first instance write to Kieran Touhey (Data Protection Officer) who has responsibility for Data Protection within our Company stating the details of your complaint. We would ask that you provide us with as much detail as possible to allow a thorough investigation. Your complaint will be acknowledged within 24 hours and we aim to resolve any complaint within 5 working days. However, depending on the complexity of the complaint and availability of external agencies it may on occasions take longer.

Should your complaint show that we have breached our duty of care we will report the breach to the Information Commissioner's Office.

If you are not satisfied by our response you may complain to the ICO.

Data Subject Access Request Procedure

1. Purpose

Care Today Children's Services / Parallel Parents Ltd ("we"/"us") have this procedure in place to provide a standardised response to any data subject access requests ("DSARs") that we receive and ensure that DSARs are appropriately managed and responded to in accordance with the law and best practice.

Data subjects have the right to request access to their personal data processed by us and are entitled to obtain:

- Confirmation that their data is being processed;·
- Access to their personal data;
- Any related information;

2. Scope

This procedure only applies to data subjects whose personal data we process.

For the purposes of this procedure, "personal data" means any information relating to an identified or identifiable data subject. An identifiable data subject is anyone who can be identified, directly or indirectly, by reference to an identifier, such as a name, identification number or online identifier. "Processing" means any operation or set of operations that is performed on personal data, such as collection, use, storage, dissemination and destruction.

3. Procedure

3.1 If you receive a DSAR direct from a data subject please forward the details onto the Data Protection Officer (Kieran Touhey)

3.2 When a data subject makes an DSAR we shall take the following steps:

(a) log the date on which the request was received to ensure that the relevant timeframe of one month (unless the DSAR is found to be excessive) for responding to the request is met;

(b) confirm the identity of the data subject who is the subject of the personal data. For example, we may request additional information from the data subject to confirm their identity;

(c) search databases, systems, applications and other places where the personal data which are the subject of the request may be held; and

(d) confirm to the data subject whether or not personal data of the data subject making the DSAR are being processed.

3.3 If personal data of the data subject are being processed, we shall provide the data subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

(a) the purposes of the processing;

(b) the categories of personal data concerned (for example, contact details, bank account information and details of sales activity);

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas (for example, US-based service providers);

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;

(f) the right to lodge a complaint with the Information Commissioner's Office (ICO);

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; and

(i) where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data.

3.4 We shall also, unless there is an exemption (see below), provide the data subject with a copy of the personal data processed by us in a commonly used electronic form (unless the data subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form) within one month of receipt of the request. If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding we shall inform the data subject within one month of receipt of the request and explain the reason(s) for the delay.

3.5 Before providing the personal data to the data subject making the DSAR, we shall review the personal data requested to see if they contain the personal data of other data subjects. If they do, we may redact the personal data of those other data subjects prior to providing the data subject with their personal data, unless those other data subjects have consented to the disclosure of their personal data.

3.6 If the DSAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data, or refuse to act on the request.

3.7 If we are not going to respond to the DSAR we shall inform the data subject of the reason(s) for not taking action and of the possibility of lodging a complaint with the ICO.

4. Exemptions

Before responding to any request we shall check whether there are any exemptions that apply to the personal data that are the subject of the request. Exemptions may apply where it is necessary and proportionate not to comply with a DSAR to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

(e) other important objectives of general national public interest, in particular an important national economic or financial interest, including monetary, budgetary and taxation matters, public health and social security;

(f) the protection of judicial independence and judicial proceedings;

(g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in (a) and (g) above;

(i) the protection of the data subject or the rights and freedoms of others; or

(j) the enforcement of civil law claims.