

Section <b>Human Resources</b>	Subject <b>GDPR Data Protection Policy - Employees</b>
Date <b>July 2022</b>	Review Date <b>01/07/2023</b>
Issuing Department <b>HR</b>	Number of Pages <b>7</b>
Applicability Code <b>All Divisions</b>	Contact <b>AMANDA WRISDALE</b>

## 1. Protecting personal data

- 1.1 Protecting personal data is very important. Whether it belongs to you or individuals we work with we take our responsibilities very seriously.
- 1.2 Not only do we need to ensure that we protect your personal data but you also need to help us to protect other personal data that we hold.
- 1.3 We have appointed a 'Data Protection Officer' to ensure that this policy is implemented appropriately. If you have any questions or concerns about this policy or the processing of personal data please speak with them first.
- 1.4 Our Data Protection Officer is Amanda Wrisdale, the Group HR Manager. ([hr@barkerross.co.uk](mailto:hr@barkerross.co.uk))

### Protecting personal data

- 1.5 When dealing with personal data there are eight principles that you and we need to follow. The personal data needs to be:
  - (a) Processed fairly and lawfully;
  - (b) Relevant and not excessive;
  - (c) Processed for limited purposes and in an appropriate way;
  - (d) Accurate;
  - (e) Not kept longer than necessary;
  - (f) Processed in accordance with the laws dealing with personal data;
  - (g) Kept secure;
  - (h) Not transferred to people or organisations in countries without adequate protection.

There is a lot to understand in respect of these principles. This policy should help you to ensure that your and our treatment of personal data is appropriate and lawful. If you have any questions, please direct them to 'Data Protection Officer'.

### A lawful purpose for processing your personal data

- 1.6 We process personal data fairly and lawfully. Grounds for processing personal data include with your consent, to comply with a legal obligation, in your vital interests, in the performance of a contract with you or in our legitimate interests (or a third party processing your personal data). If the personal data is sensitive additional conditions will be met.
- 1.7 At the end of this policy we identify the categories of personal data that we collect and the reasons for processing it along with a privacy notice explaining more about what we do with your personal data.
- 1.8 Where we process the following data, we will secure your consent before doing so:
  - (a) personal data about your health to:
    - (i) monitor sick leave; and
    - (ii) take decisions as to your fitness for work;
  - (b) processing personal data to meet with our legal obligations to third parties including pensions and insurance providers;
  - (c) processing personal data to measure and manage equal opportunities;
  - (d) transferring your personal data to a country outside of the European Economic Area provided that we are satisfied with the protections that they have in place to protect your data (unless it's a one off transfer of data);
  - (e) sharing your personal data with a company within our group (where applicable) or with any person or business that intends to buy us or take over control;
  - (f) sharing your personal data with the Fit For Work Service, your doctor, consultant and/or occupational health specialist;
  - (g) sharing your personal information with the Disclosure and Barring Service (or equivalent).

### **Requests to see your personal data**

- 1.9 If you want us to show you personal data that we hold on you then you need to make a request in writing to the 'Data Protection Officer'. We might ask you for more details about the request or give you a template letter to help with your request. Where the request isn't made in person we will always ask for two forms of identity to confirm that it is you making the request.
- 1.10 We'll always try and acknowledge your request when we receive it. We've got between 30 days and three months to respond in full to your request.
- 1.11 We may ask you to contribute towards the administration fee in processing your request.
- 1.12 If you are asked to disclose personal data you should notify the Data Protection Officer' immediately and follow their instructions.

### **Your rights to deletion, freezing data processing and corrections**

- 1.13 You can ask us to delete your personal data where:
  - (a) Processing it is no longer necessary bearing in mind the reason it was collected;
  - (b) It is being processed unlawfully;
  - (c) You object to us processing your personal data (unless we have an over-riding legitimate interest for continuing to process it in which case we may continue to do so).
- 1.14 Where information we hold on you is inaccurate or incomplete you can ask us rectify the data.
- 1.15 You can ask us to stop processing your data where:
  - (a) Processing is unlawful;
  - (b) You say that the information that we hold is inaccurate;
  - (c) You don't consider we have a 'legitimate interest' for processing the data (unless we have an over-riding legitimate interest for continuing to process it in which case we will continue to do so).
- 1.16 If we think that you're abusing these rights and making unfounded or excessive requests, we may refuse your request or may charge a reasonable administration fee for processing the request.

### **Limitations and obligations**

- 1.17 We have processes in place to ensure that the accuracy of the personal data that we hold is up to date. Obviously, if personal data that we hold on you is out of date or inaccurate please notify the Data Protection Officer. We will talk to you at least once a year and at the point that you leave our employment about the personal data that we hold on you, whether it is still necessary to hold that data and whether any of it is inaccurate or out of date.
- 1.18 Wherever possible you should always encrypt personal data so that it is not easily accessible to others. Equally, you and we should not capture more personal data than is needed for the purpose identified. Where you are able to anonymise personal data you are encouraged to do so.
- 1.19 We will retain your personal data in accordance with our 'policy on retaining your personal data'. We have processes in place to ensure that personal data isn't kept for longer than necessary. Once it's no longer necessary for processing purposes we will delete it.
- 1.20 We have put appropriate security measures in place to stop accidental loss of, or damage to personal data. Where we have shared with you those measures you must comply with them. Where we ask third parties to process your personal data we will ensure that they have appropriate security measures in place too and that they comply with data protection legislation.
- 1.21 Bear in mind that desks and equipment hold personal data. You should keep locked away or password protected any personal data and such data should be kept out of view of others at all times. Please ensure that you comply with our 'email, the internet and our equipment' policy and our 'clear desk' policies along with other relevant policies.
- 1.22 A data breach is a breach of data security that leads to accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data. It includes sending emails to the wrong person, carelessness with passwords and leaving personal data on desks. If you become aware of a data breach you should immediately notify the Data Protection Officer.
- 1.23 Usually, we will only process or share your personal data for the purpose it was collected. So, if it was gathered as part of a discussion about a medical condition that you have then generally we will not use the information for any other reason. Sometimes, in processing personal data we become aware of information that we cannot ignore, even if it means using it for a purpose beyond the reason it was collected. For example, if we use CCTV for health and safety reasons and happen upon misconduct we are not expected to ignore that. Where that is the case, we will confirm the extended use of the personal data.

- 1.24 If you become aware that personal data has become lost, stolen or otherwise transferred outside of Barker Ross Group accidentally or without authorisation, you need to report this immediately to the Data Protection Officer.
- 1.25 If you breach this policy that will be dealt with under our disciplinary policy.
- 1.26 This policy may be changed from time to time. We will notify you of any changes.

#### Information about your data

Type of data	Relevant privacy notice	Reason for processing the data	Type of processing	Who processes the data	Where the data came from	Any recipients of the data
Your name	attached	identification	contractual	Barker Ross Group	you	Our insurers
Your address, your cv, your bank account and NI details, personal contact details	attached	identification	contractual	Barker Ross Group	you	Our insurers
Next of kin details	attached	Information, health and safety	Health and safety	Barker Ross Group	you	n/a
Right to work information, including passport, long birth certificate, biometric residence card or EEA national ID card	attached	legislative	Legislative, to demonstrate evidence of the right to work	Barker Ross Group	you	n/a
Sick note / return to work forms	attached	legislative	Legislative, to confirm sickness / confirmation of fitness to work	Barker Ross Group	you	n/a
Maternity / paternity forms	attached	legislative	Legislative / to confirm statutory benefit	Barker Ross Group	you	n/a
Driving licence (drivers only)	attached	Legislative / contractual	To confirm that you hold a current licence (required for those that are to drive company vehicles only)	Barker Ross Group	you	DVLA (to complete DVLA checks)
DVLA checks	attached	Legislative / contractual	To confirm that your licence is current	Barker Ross Group	DVLA	n/a
Salary sacrifice confirmation	attached	contractual	Only applicable for those that have opted to take a salary sacrifice (childcare vouchers, for example)	Barker Ross Group	you	Salary sacrifice scheme providers
Insurance (Health / Life, etc)	attached	contractual	Only applies to those that qualify for Health insurance	Barker Ross Group	you	Health insurance providers
DBS checks / caution / conviction history	attached	legislative	Only applies if your role requires you to come into contact with vulnerable adults or children	Barker Ross Group	you	U Check



## **Privacy notice: Employees**

### **Our commitment to your privacy**

We're serious about protecting your personal data. This note explains:

- From where we secured your personal data;
- The personal data that we collect;
- Your personal data rights;
- Your right to object to our processing your personal data and withdrawing consent;
- How and when we use that personal data;
- Whether we share your personal data with anyone else;
- For how long will we keep your personal data;
- How you can access your personal data
- Information about our use of cookies.

If you have any questions or queries about this notice please email us at [dpo@barkerross.co.uk](mailto:dpo@barkerross.co.uk)

### **Personal data that we collect**

The personal data that we collect includes your name, address, email address, telephone number, mobile phone number, proof of right to work documents and data, bank account, training and qualifications, trade memberships, preferences, IP address (the number that uniquely identifies a specific computer).

If the role you have registered for requires a security check, we will also obtain a DBS check provided by you.

We collected your personal data from you. We also collected the following personal data from third parties:

- example – your reference was secured from your previous employer, agency or Character reference;

We always ensure that we have a lawful basis for processing the personal data that we collect. In this case the lawful basis for processing is to offer work finding services.

### **Your rights in respect of your personal data**

You have the right to request access to your personal data, amendments to it and for it to be deleted. Further information about those rights along with your right to withdrawn any consent you've given or object to our processing your data can be found in our data protection policy. That policy also includes who to speak with if you have any queries about our approach to processing your personal data.

### **How and when we use your personal data**

We're committed to using your personal data responsibly and lawfully. Here's what we do with your personal data:

- Your HR information is retained in line with your employment;
- Processing your salary.

Your personal data is all stored within the UK.

To help us to maintain the accuracy of the personal data that we hold please let us know if we hold out of date or inaccurate information about you.

**Sharing your personal data**

There are only a few occasions where we will share your personal data with a third party. They are:

- example – where we're required to disclose it by law – to government bodies for example;
- example - between ourselves – for example to deal with a query that you may have; example – your reference was secured from your previous employer;
- example – medical information was provided to us from our health check providers.
- Example – DVLA checks, where you are authorised to drive a company supplied vehicle
- Example – DBS checks, where you may come into contact with vulnerable adults or children as part of your role.

There may be occasions where you will be requested to share your personal details to have a key fob, entry card or biometric scan, such as a finger print. Such information will only be used to allow you access to a client site. Where this is the case, you will be informed in advance and be required to consent to such data being shared separately.

The data controller collecting your personal data for the purpose of this policy is Barker Ross Group Limited and its Group Companies; Barker Ross Staffing Solutions Limited, Barker Ross Recruitment Limited and Cardea Resourcing Limited, T/A Barker Ross Health and Social Care. We use accepted standards of technology and security to protect your personal data.

**For how long will we keep your personal data**

Our 'retention policy' lists the type of data we process and for how long it is kept. You can access that policy by reviewing the Retention policy below.. If you would like us to delete your data and we don't have a lawful reason to retain it you can make a

deletion request by writing to The Data Protection Officer, Barker Ross Group, Mercury Place, 11 St George Street, Leicester, LE1 1QG.

#### How you can access your personal data

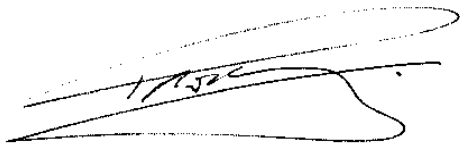
You can ask us for a copy of the personal data that we hold on you by writing to The Data Protection Officer, Barker Ross Group, Mercury Place, 11 St George Street, Leicester, LE1 1QG. We'll ask you for copies of two types of approved identity in order to process your request (such as a passport and driving licence). You can also ask us to make corrections to data you consider to be inaccurate by writing to The Data Protection Officer, Barker Ross Group, Mercury Place, 11 St George Street, Leicester, LE1 1QG.

#### Our policy on retaining your personal data

Here's a note of some of the personal data that we hold and for how long we keep it.

Personal data	Period held
Job applications and interview records	Six months if unsuccessful  If you're happy for us to retain your data for future opportunities we'll confirm how long we'll keep it at the point that you give us the information
'Right to work' checks	Two years after employment ends
Time sheets and Working Time Regulations opt-outs	Two and a half years
Records relating to maternity leave and maternity pay (and other family leave and pay)	Three years after the end of the tax year in which family related leave ended
Records relating to any accident, death or injury in connection with work	Three years from the date of the incident, or if anyone injured was under 18, three years from their eighteenth birthday
Employment files, including: <ul style="list-style-type: none"> <li>• Application, CV and details of previous employment</li> <li>• Next of kin/emergency contact info</li> <li>• Contact of employment</li> <li>• References given and received</li> <li>• Qualifications and checks with professional bodies</li> <li>• Annual reviews</li> <li>• Disciplinary/grievance records</li> <li>• Sickness absence records</li> <li>• Training records</li> <li>• Employment related correspondence</li> <li>• Subject access requests and responses</li> <li>• Consent for the processing of data</li> <li>• Driving licence and insurance data</li> <li>• Records of any advances or loans</li> <li>• Pension information</li> </ul>	During your employment and six years after

Holiday records	Six years, or longer if any annual leave was carried over from previous years
Payroll records	Six years from financial year end
Collective workforce agreements and works council meeting minutes	Permanently
Bank details	During your employment and six years after
Equal opportunities monitoring data	During employment and six years after
DBS certificate	For unsuccessful applicants, deleted immediately. Only kept during employment where relevant to the role and conviction remains unspent. Certificates should be deleted once a conviction becomes spent, unless the role allows you to carry out full DBS checks.
Records of criminal convictions	Deleted as soon as the conviction is spent, unless working in an exempt profession
Death benefit nomination and revocation forms	During employment (and if any payments are made, six years after the last payment of benefit)
IP addresses, internet usage history, recorded calls and location data from company equipment	Six years
General commercial personal data – e.g. sales information, client data	Six years
Court/tribunal papers	Six years
Photos	During your employment and six years after
Trade union agreements	Permanently



Paul Ross  
**Group Chief Executive**  
 For and on behalf of  
**Barker Ross Group**  
 July 2022