**Privacy**

Protecting your privacy and personal information is taken very seriously by us. Unfortunately, there may be individuals pretending to be employees of Black Cat Recruitment Ltd or any of our associated trading names, who may try to obtain your information fraudulently:

* The BlackCat Talent Co.
* BlackCat Recruitment
* BlackCat Recruitment Club
* BlackCat Futures

Be cautious when opening or responding to e-mails from anyone claiming to be from or representing Black Cat Recruitment Ltd, The BlackCat Talent Co., BlackCat Recruitment, BlackCat Futures or BlackCat Recruitment Club. If you’re not sure if you’re being contacted by a genuine member of Black Cat Recruitment Ltd or our Payroll Providers Simplicity or GAIN, there are two quick safety checks you can make:

Any e-mail from our employees will feature an email address using one of the following formats:

firstname@blackcatrecruitment.co.uk

firstname@blackcattalent.co.uk

Or from our Payroll Providers:

firstname.surname@simplictyinbusiness.com

payroll@simplicityinbusiness.com

firstname.surname@gainadvantage.org

admin@gainadvantage.org

Call the Directors of The BlackCat Talent Co. to ask if the communication is genuine, directly on:

0121 368 1500 (Landline)

07718 964 585 (Ian Shuttleworth)

07767 279 451 (Saran Cliff)

If you receive any emails or communication from any other accounts or personnel claiming to be representing The Black Cat Recruitment Company or Black Cat Recruitment Ltd, please report this to your e-mail provider and do NOT provide any information until you are confident that the communication is genuine.

**Our Privacy Policy:**

The Company is a recruitment business which provides work-finding services to its clients and work-seekers. The Company must process personal data (including sensitive personal data) so that it can provide these services – in doing so, the Company acts as a data controller.

You may give your personal details to the Company directly, such as on an application or registration form or via our website, or we may collect them from another source such as a jobs board. The Company must have a legal basis for processing your personal data. For the purposes of providing you with work-finding services and/or information relating to roles relevant to you we will only use your personal data in accordance with this privacy statement. At all times we will comply with current data protection laws.

**Contents**

* Collection and use of personal data
* Purpose of processing and legal basis
* Legitimate interest
* Statutory/contractual requirement
* Recipients of data
* Information to be provided when data is not collected directly from the data subject
* Categories of data
* Sources of data
* Overseas transfers
* Data retention
* Your rights
* Automated decision making
* Cookies
* Login files
* Links to external sites
* Sale of the business
* Data security
* Changes to this privacy statement

**Complaints or Queries**

* Collection and use of personal data
* Purpose of processing and legal basis

The Company will collect your personal data (which may include sensitive personal data) and will process your personal data for the purposes of providing you with work-finding services. This includes for example, contacting you about job opportunities, assessing your suitability for those opportunities, updating our databases, putting you forward for job opportunities, arranging payments to you and developing and managing our services and relationship with you and our clients.

In some cases, the Company may be required to use your data for the purpose of investigating, reporting and detecting crime and also to comply with laws that apply to us. We may also use your information during the course of internal audits to demonstrate our compliance with certain industry standards.

We must have a legal basis to process your personal data. The legal bases we rely upon to offer our work-finding services to you are:

* Your consent
* A legitimate interest to process your data

**Legitimate Interest**

This is where the Company has a legitimate reason to process your data provided it is reasonable and does not go against what you would reasonably expect from us. Where the Company has relied on a legitimate interest to process your personal data our legitimate interests is/are as follows:

* Managing our database and keeping work-seeker records up to date;
* Providing work-finding services to you and our clients;
* Contacting you to seek your consent where we need it;
* Managing our database and keeping work-seeker records up to date;
* Contacting individuals to seek consent to provide work-finding services;
* Providing work-finding services to the individual, including sending personal information to prospective clients where a demonstration of an interest has been shown in doing that particular type of work, but has not expressly consented to us passing on your cv;
* Contacting individuals with information about similar job roles that may suit their experience; and
* Passing work-seeker’s information to debt collection agencies as required by law
* To comply with the legal obligation that we have to ensure work-seekers have the right to work in the UK
* To fulfil a statutory/contractual obligation that you have the required qualifications or training to carry out a certain job role or task

**Statutory/contractual Requirement**

The Company has certain legal and contractual requirements to collect personal data (e.g. to comply with the Conduct of Employment Agencies and Employment Businesses Regulations 2003, immigration and tax legislation, and in some circumstances safeguarding requirements.) Our clients may also require this personal data, and/or we may need your data to enter into a contract with you. If you do not give us personal data we need to collect we may not be able to continue to provide work-finding services to you.

**Recipient/s of Data**

The Company will process your personal data and/or sensitive personal data with the following recipients:

* Prospective Employers / Clients (with whom we may introduce or supply you to)
* Former employers whom we may seek references from
* Keen Thinking Ltd T/A Simplicity and GAIN payroll service providers who manage payroll on our behalf
* Keen Thinking Ltd T/A Simplicity, GAIN & GEMS CRM database provider to store your information if you commence work with the Company
* Other recruitment agencies in our supply chain should you engage in work with a client we are supplying via another Recruitment / Employment Provider in a Managed Service or Second Tier capacity

Information to be provided when data collected not from the data subject]

Categories of data: The Company may collect the following personal data on you:

* Full Name,
* Home Address
* Telephone & mobile number/s
* E-mail Address
* National Insurance Number
* Date of Birth
* Nationality (through our eligibility to work in the UK checks)
* Employment History
* Next of Kin Name & Contact Information
* Education & Qualification details

**Sensitive Personal Data:**

* [Health information including whether you have a disability]
* [Criminal convictions]
* Bank Details (if you are employed on a temporary basis)

**Source of the Personal Data:**

The Company may source your personal data/sensitive personal data from:

* LinkedIn, Jobsite, Total Jobs, Facebook, Instagram, Twitter, Indeed, Universal JobMatch, Fish4, Monster, CV Library, Reed, Public Domain Internet Search Engines e.g. Google, Yahoo etc.
* A referee whose details you previously provided to us (personal or employer)
* Software provides who we use to support our services including GEMS CRM
* Cookies listed in section 7
* This information [came/did not come] from a publicly accessible source.
* Overseas Transfers
* The Company will not transfer the information you provide to us to countries outside the European Economic Area (‘EEA’) for the purposes of providing you with work-finding services. The EEA comprises the EU member states plus Norway, Iceland and Liechtenstein.

**Data Retention**

The Company will retain your personal data only for as long as is necessary for the purpose we collect it. Different laws may also require us to keep different data for different periods of time. For example, the Conduct of Employment Agencies and Employment Businesses Regulations 2003, require us to keep work-seeker records for at least one year from (a) the date of their creation or (b) after the date on which we last provide you with work-finding services.

We must also keep your payroll records, holiday pay, sick pay and pensions auto-enrolment records for as long as is legally required by HMRC and associated national minimum wage, social security and tax legislation. This is currently 3 to 6 years.

Where the Company has obtained your consent to process your [personal/[and] sensitive personal data, we will do so in line with our retention policy (a copy of which is available to view on our Company website: www.blackcatrecruitment.co.uk). Upon expiry of that period the Company will seek further consent from you. Where consent is not granted the Company will cease to process your personal/and / or] sensitive data.

**Your Rights**

Please be aware that you have the following data protection rights:

* The right to be informed about the personal data the Company processes on you;
* The right of access to the personal data the Company processes on you;
* The right to rectification of your personal data;
* The right to erasure of your personal data in certain circumstances;
* The right to restrict processing of your personal data;
* The right to data portability in certain circumstances;
* The right to object to the processing of your personal data that was based on a public or legitimate interest;
* The right not to be subjected to automated decision making and profiling; and
* The right to withdraw consent at any time.

Where you have consented to the Company processing your personal [and/or] sensitive personal data you have the right to withdraw that consent at any time by contacting Ian Shuttleworth – Director (via e-mail: ian@blackcatrecruitment.co.uk)or Saran Cliff – Director (via e-mail: saran@blackcattalent.co.uk). Please note that if you withdraw your consent to further processing that does not affect any processing done prior to the withdrawal of that consent, or which is done according to another legal basis.

There may be circumstances where the Company will still need to process your data for legal or official reasons. Where this is the case, we will tell you and we will restrict the data to only what is necessary for those specific reasons.

If you believe that any of your data that the Company processes is incorrect or incomplete, please contact us using the details above and we will take reasonable steps to check its accuracy and correct it where necessary.

You can also contact us using the above details if you want us to restrict the type or amount of data we process for you, access your personal data or exercise any of the other rights listed above.

**Automated Decision-Making**

On occasion, the Company may utilise the automated decision-making of job advertising or CV hosting websites based on questions set by the Company relating to suitability for individual job roles advertised. Questions asked are required to determine the eligibility of the job-seeker to carry out the job role i.e. “Do you have a current Driving Licence?” If the job-seeker were to answer “No” and the position required a valid Driving Licence to undertake the role i.e. a Driving position, then the job-seeker would be rejected.

**Cookies**

We may obtain data about you from cookies. These are small text files that are placed on your computer by websites that you visit. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. Cookies also enable us to deliver more personalised content.

Most web browsers allow some control of most cookies through the browser settings. To find out more about cookies, [please refer to our Cookie policy]. [Please note that in a few cases some of our website features may not function if you remove cookies from your browser.]

**Log Files**

We use IP addresses to analyse trends, administer the site, track users’ movements, and to gather broad demographic information for aggregate use. IP addresses are not linked to personally identifiable information.

**Links to External Websites**

The Company’s website may contain links to other external websites. Please be aware that the Company is not responsible for the privacy practices of such other sites. When you leave our website, we encourage you to read the privacy statements of each and every website that collects personally identifiable information. This privacy statement applies solely to information collected by the Company’s website (www.blackcattalent.co.uk)

**Sale of Business**

If the Company’s business is sold or integrated with another business your details may be disclosed to our advisers and any prospective purchasers and their advisers and will be passed on to the new owners of the business.

**Data Security**

The Company takes every precaution to protect our users’ information. e.g. firewalls, browser certification technology, encryption, limited access, use of passwords to access any sensitive information on all Computer and Handheld Device Technology used to hold data.

Only employees and authorised external organisations who need the information to perform a specific job (for example, payroll (Keen Thinking Ltd T/A Simplicity) is granted access to your information.

The Company uses all reasonable efforts to safeguard your personal information. However, you should be aware that the use of email/ the Internet is not entirely secure and for this reason the Company cannot guarantee the security or integrity of any personal information which is transferred from you or to you via email/ the Internet.

If you share a device with others we recommend that you do not select the “remember my details” function when that option is offered.

If you have any questions about the security at our website, you can email Ian Shuttleworth – Director at: ian@blackcatrecruitment.co.uk or Saran Cliff – Director at: saran@blackcattalent.co.uk

**Changes to this Privacy Statement**

We will update this privacy statement from time to time. We will post any changes on the statement with revision dates. If we make any material changes, we will notify you.

**Complaints or Queries**

If you wish to complain about this privacy notice or any of the procedures set out in it please contact Ian Shuttleworth – Director at: ian@blackcatrecruitment.co.uk or Saran Cliff – Director at: saran@blackcattalent.co.uk

You also have the right to raise concerns with Information Commissioner’s Office on: 0303 123 1113 or at <https://ico.org.uk/concerns/> or any other relevant supervisory authority should your personal data be processed outside of the UK. If you believe that your data protection rights have not been adhered to.

**Our Data Protection Procedure:**

Contents table:

* Introduction
* Definitions
* Data processing under the Data Protection Laws
* Information security
* Rights of the individual
* The right to be informed
* The right to access (‘subject access request’)
* The right to rectification
* The right to erasure (‘the right to be forgotten’)
* The right to restrict processing
* The right to data portability
* The right to object to processing
* Automated decision-making processes
* The right to withdraw consent
* Timing and information to be provided to the individual
* Charges
* Personal data breaches
* Record keeping
* Complaints
* Appendix
* Annex A

**Introduction**

All organisations that process personal data are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the ‘Data Protection Laws’). The Data Protection Laws give individuals (known as ‘data subjects’) certain rights over their personal data whilst imposing certain obligations on the organisations that process their data.

As a Recruitment Business the Company collects and processes both personal data and sensitive personal data. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

This policy sets out how the Company implements the Data Protection Laws. It should be read in conjunction with the “Data Protection Procedure”.

**Definitions**

In this policy the following terms have the following meanings:

* *‘consent’* means any freely given, specific, informed and unambiguous indication of an individual’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of persona data relating to him or her;
* *‘data controller’* means an individual or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data;
* *‘data processor’* means an individual or organisation which processes personal data on behalf of the data controller;
* *‘personal data’* \* means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
* *‘personal data breach’* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;
* *‘processing’* means any operation or set of operations performed on personal data, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
* *‘profiling’* means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
* *‘pseudonymisation’* means the processing of personal data in such a manner that the personal data can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;
* *‘sensitive personal data’* \* means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data,
* biometric data, data concerning health, an individual’s sex life or sexual orientation and an individual’s criminal convictions.
* For the purposes of this policy we use the term ‘*personal data*’ to include ‘*sensitive personal data*’ except where we need to refer to *sensitive personal data* specifically.
* *‘Supervisory authority’* means an independent public authority which is responsible for monitoring the application of data protection. In the UK the supervisory authority is the Information Commissioner’s Office (ICO).

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

**Data Processing under the Data Protection Laws**

The Company processes personal data in relation to its own staff, work-seekers and individual client contacts and is a data controller for the purposes of the Data Protection Laws. The Company has registered with the ICO and its registration number is ZA309105.

The Company may hold *personal data* on individuals for the following purposes:

* Staff administration;
* Advertising, marketing and public relations;
* Accounts and records;
* Administration and processing of work-seekers’ personal data for the purposes of providing work-finding services, including processing using software solution providers and back office support and:
* Administration and processing of clients’ personal data for the purposes of supplying/introducing work-seekers
* The Company will only process personal data where it has a legal basis for doing so (see Annex A). Where the Company does not have a legal reason for processing personal data any processing will be a breach of the Data Protection Laws.

**Information Security**

Only those listed in the Appendix are permitted to add, amend or delete personal data from the Company’s database(s) (‘database’ includes paper records or records stored electronically).

* All Company staff are responsible for notifying those listed in the Appendix where information is known to be old, inaccurate or out of date or a request for erasure, access, rectification or restriction of *processing* has been received from the individual.
* Company staff are also responsible for notifying those listed in the Appendix where any request for data portability, objection to *processing* or where *consent* to process has been withdrawn and has been received from the individual.
* The incorrect *processing* of *personal data* e.g. sending an individual’s details to the wrong person, allowing unauthorised persons access to personal data, sending information out for purposes for which the individual did not give their *consent*, or not having a lawful reason to process personal data, may give rise to a breach of contract and/or negligence leading to a claim against the Company for damages from an employee, work-seeker or client contact.

In addition, all Company staff should ensure that adequate security measures are in place to limit the risk of *personal data breaches*. For example:

* Staff should lock their computer screens when they are not in use.
* All devices, whether company or personal devices (including but not limited to computers, mobile phones, other hand-held devices) containing personal data relating to the services of the Company shall be encrypted and password protected.
* Staff should not disclose their passwords to anyone
* Email should be used with care. Company staff must ensure that emails are sent only to the intended recipient/s.
* Where Company staff send an email in error then the email must be recalled immediately, and Company staff must inform those listed in the Appendix of the error so that any risk of a personal data breach can be limited.
* Personnel files (whether for internal staff or work-seekers) and other personal data should be stored securely to prevent unauthorised access. They should not be removed from their usual place of storage without good reason.
* Personnel files (whether for internal staff or work-seekers) should always be locked away when not in use and when in use should not be left unattended.
* Personal data should only be stored for the periods set out in the Company’s data retention policy.
* Processing includes the destruction or disposal of personal data. Therefore, staff should take care to destroy or dispose of personal data safely and securely. Such material should be shredded or stored as confidential waste awaiting safe destruction.

**Rights of the Individual**

An individual has the following rights under the Data Protection Laws:

* The right to be informed of what information the Company holds on them – this is typically given to the individual in a privacy notice;
* The right of access to any personal data that the Company holds on them – this is usually referred to as a ‘subject access request’;
* The right to rectification of personal data that the individual believes is either inaccurate or incomplete;
* The right to erasure of their personal data in certain circumstances;
* The right to restrict *processing* of their personal data;
* The right to data portability of their personal data in specific circumstances;
* The right to object to the *processing* of their personal data where it is based on either a legitimate interest or a public interest;
* The right not to be subjected to automated decision making and *profiling*; and
* The right to withdraw *consent* where it was relied upon to process their personal data.
* The right to be informed
* Any individual whose *personal data* is processed by the Company will have the right to be informed about such *processing*. They will have the right to be informed about who, what, where and why the data is processed. This information should be delivered in a privacy notice, in writing and where appropriate electronically. Depending on where the personal data are being collected, an individual may be directed to the Company’s website privacy notice or be given a copy of a privacy notice.

This privacy notice should be issued in instances where either:

* the Company collects/processes data directly from the individual; or
* the Company has not collected/processed the data from the individual directly.
* The privacy notice should include the information set out in Table 1 (below).

In addition:

Where personal data has been collected from the individual the privacy notice will need to be issued at the point the data is collected. Where the Company intends to further process the personal data for a purpose other than that for which the personal data was collected, the Company shall provide the individual, prior to that further *processing*, with information on that other purpose and with any relevant further information in a new updated privacy notice.

Where personal data has not been obtained from the individual, the Company shall provide the privacy notice within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed. If the personal data are to be used to communicate with the individual then the privacy notice will be issued at the time of the first communication with the individual. If a disclosure to another recipient is envisaged, then the privacy notice will be issued to the individual at the latest when the personal data are first disclosed.

Company staff will be responsible for issuing privacy notices to individuals whose personal data is processed by the Company in the timeframes and circumstances mentioned above.

**Our Data Protection Policy:**

* Contents
* Introduction
* Definitions
* Data processing under the Data Protection Laws
* The data protection principles
* Legal bases for processing
* Privacy by design and by default
* Rights of the Individual
* Privacy notices
* Subject access requests
* Rectification
* Erasure
* Restriction of processing
* Data portability
* Object to processing
* Enforcement of rights
* Automated decision making
* Personal data breaches
* Personal data breaches where the Company is the data controller
* Personal data breaches where the Company is the data processor
* Communicating personal data breaches to individuals
* The Human Rights Act 1998
* Complaints
* Appendix
* Annex – legal bases for processing personal data

**Introduction**

All organisations that process personal data are required to comply with data protection legislation. This includes in particular the Data Protection Act 1998 (or its successor) and the EU General Data Protection Regulation (together the ‘Data Protection Laws’). The Data Protection Laws give individuals (known as ‘data subjects’) certain rights over their personal data whilst imposing certain obligations on the organisations that process their data.

As a recruitment business the Company collects and processes both personal data and sensitive personal data. It is required to do so to comply with other legislation. It is also required to keep this data for different periods depending on the nature of the data.

This policy sets out how the Company implements the Data Protection Laws. It should be read in conjunction with the “Data Protection Procedure”.

**Definitions**

In this policy the following terms have the following meanings:

* ‘consent’ means any freely given, specific, informed and unambiguous indication of an individual’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of persona data relating to him or her;
* ‘data controller’ means an individual or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data;
* ‘data processor’ means an individual or organisation which processes personal data on behalf of the data controller;
* ‘personal data’ \* means any information relating to an individual who can be identified, such as by a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
* ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data;
* ‘processing’ means any operation or set of operations performed on personal data, such as collection, recording, organisation, structuring, storage (including archiving), adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
* ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
* ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to an individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;
* ‘sensitive personal data’ \* means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data,
* biometric data, data concerning health, an individual’s sex life or sexual orientation and an individual’s criminal convictions.

\* For the purposes of this policy we use the term ‘personal data’ to include ‘sensitive personal data’ except where we specifically need to refer to sensitive personal data.

‘Supervisory authority’ means an independent public authority which is responsible for monitoring the application of data protection. In the UK the supervisory authority is the Information Commissioner’s Office (ICO).

All of these definitions are italicised throughout this policy to remind the reader that they are defined terms.

**Data Processing under the Data Protection Laws**

The Company processes personal data in relation to its own staff, work-seekers and individual client contacts and is a data controller for the purposes of the Data Protection Laws. The Company has registered with the ICO and its registration number is: ZA309105.

The Company may hold personal data on individuals for the following purposes:

* Staff administration;
* Advertising, marketing and public relations;
* Accounts and records;
* Administration and processing of work-seekers’ personal data for the purposes of providing work-finding services, including processing using software solution providers and back office support and:
* Administration and processing of clients’ personal data for the purposes of supplying/introducing work-seekers

**The Data Protection Principles**

The Data Protection Laws require the Company acting as either data controller or data processor to process data in accordance with the principles of data protection. These require that personal data is:

* Processed lawfully, fairly and in a transparent manner;
* Collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
* Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
* Accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
* Kept for no longer than is necessary for the purposes for which the personal data are processed;
* Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; and that
* The data controller shall be responsible for, and be able to demonstrate, compliance with the principles.

**Legal Basis for Processing**

The Company will only process personal data where it has a legal basis for doing so (see Annex A). Where the Company does not have a legal reason for processing personal data any processing will be a breach of the Data Protection Laws.

The Company will review the personal data it holds on a regular basis to ensure it is being lawfully processed and it is accurate, relevant and up to date and those people listed in the Appendix shall be responsible for doing this.

Before transferring personal data to any third party (such as past, current or prospective employers, suppliers, customers and clients, intermediaries such as umbrella companies, persons making an enquiry or complaint and any other third party (such as software solutions providers and back office support)), the Company will establish that it has a legal reason for making the transfer.

**Privacy by Design and by Default**

The Company has implemented measures and procedures that adequately protect the privacy of individuals and ensures that data protection is integral to all processing activities. This includes implementing measures such as:

data minimisation (i.e. not keeping data for longer than is necessary);

* pseudonymisation;
* anonymization;
* cyber security;
* physical security (i.e. keeping physical data in a locked area when not in use)

The Company shall provide any information relating to data processing to an individual in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. The Company may provide this information orally if requested to do so by the individual.

**Rights of the Individual - Privacy Notices**

Where the Company collects personal data from the individual, the Company will give the individual a privacy notice at the time when it first obtains the personal data.

Where the Company collects personal data other than from the individual directly, it will give the individual a privacy notice within a reasonable period after obtaining the personal data, but at the latest within one month. If the Company intends to disclose the personal data to a third party, then the privacy notice will be issued when the personal data are first disclosed (if not issued sooner).

Where the Company intends to further process the personal data for a purpose other than that for which the data was initially collected, the Company will give the individual information on that other purpose and any relevant further information before it does the further processing.

**Subject Access Requests**

The individual is entitled to access their personal data on request from the data controller.

**Rectification**

The individual or another data controller at the individual’s request, has the right to ask the Company to rectify any inaccurate or incomplete personal data concerning an individual.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to rectify the personal data unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold – however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

**Erasure**

The individual or another data controller at the individual’s request, has the right to ask the Company to erase an individual’s personal data.

If the Company receives a request to erase it will ask the individual if s/he wants his personal data to be removed entirely or whether s/he is happy for his or her details to be kept on a list of individuals who do not want to be contacted in the future (for a specified period or otherwise). The Company cannot keep a record of individuals whose data it has erased so the individual may be contacted again by the Company should the Company come into possession of the individual’s personal data at a later date.

If the Company has made the data public, it shall take reasonable steps to inform other data controllers and data processors processing the personal data to erase the personal data, taking into account available technology and the cost of implementation.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to erase the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold – however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

**Restriction of Processing**

The individual or a data controller at the individual’s request, has the right to ask the Company to restrict its processing of an individual’s personal data where:

* The individual challenges the accuracy of the personal data;
* The processing is unlawful, and the individual opposes its erasure;
* The Company no longer needs the personal data for the purposes of the processing, but the personal data is required for the establishment, exercise or defence of legal claims; or
* The individual has objected to processing (on the grounds of a public interest or legitimate interest) pending the verification whether the legitimate grounds of the Company override those of the individual.

If the Company has given the personal data to any third parties it will tell those third parties that it has received a request to restrict the personal data, unless this proves impossible or involves disproportionate effort. Those third parties should also rectify the personal data they hold – however the Company will not be in a position to audit those third parties to ensure that the rectification has occurred.

**Data Portability**

The individual shall have the right to receive personal data concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and have the right to transmit those data to another data controller in circumstances where:

The processing is based on the individual’s consent or a contract; and

The processing is carried out by automated means.

Where feasible, the Company will send the personal data to a named third party on the individual’s request.

**Object to Processing**

The individual has the right to object to their personal data being processed based on a public interest or a legitimate interest.

The individual will also be able to object to the profiling of their data based on a public interest or a legitimate interest.

The Company shall cease processing unless it has compelling legitimate grounds to continue to process the personal data which override the individual’s interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

The individual has the right to object to their personal data being used for direct marketing.

**Enforcement of Rights**

All requests regarding individual rights should be sent to the person whose details are listed in the Appendix.

The Company shall act upon any subject access request, or any request relating to rectification, erasure, restriction, data portability or objection or automated decision-making processes or profiling within one month of receipt of the request. The Company may extend this period for two further months where necessary, taking into account the complexity and the number of requests.

Where the Company considers that a request under this section is manifestly unfounded or excessive due to the request’s repetitive nature the Company may either refuse to act on the request or may charge a reasonable fee taking into account the administrative costs involved.

**Automated Decision Making**

The Company will not subject individuals to decisions based on automated processing that produce a legal effect or a similarly significant effect on the individual, except where the automated decision:

Is necessary for the entering into or performance of a contract between the data controller and the individual;

Is authorised by law; or

The individual has given their explicit consent.

The Company will not carry out any automated decision-making or profiling using the personal data of a child.

**Personal Data Breaches**

All data breaches should be referred to the persons whose details are listed in the Appendix.

Personal data breaches where the Company is the data controller:

Where the Company establishes that a personal data breach has taken place, the Company will take steps to contain and recover the breach. Where a personal data breach is likely to result in a risk to the rights and freedoms of any individual the Company will notify the ICO.

Where the personal data breach happens outside the UK, the Company shall alert the relevant supervisory authority for data breaches in the effected jurisdiction.

Personal data breaches where the Company is the data processor:

* The Company will alert the relevant data controller as to the personal data breach as soon as they are aware of the breach.
* Communicating personal data breaches to individuals
* Where the Company has identified a personal data breach resulting in a high risk to the rights and freedoms of any individual, the Company shall tell all affected individuals without undue delay.
* The Company will not be required to tell individuals about the personal data breach where:
* The Company has implemented appropriate technical and organisational protection measures to the personal data affected by the breach, in particular to make the personal data unintelligible to any person who is not authorised to access it, such as encryption.
* The Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of the individual is no longer likely to materialise.
* It would involve disproportionate effort to tell all affected individuals. Instead, the Company shall make a public communication or similar measure to tell all affected individuals.

**The Human Rights Act 1998**

All individuals have the following rights under the Human Rights Act 1998 (HRA) and in dealing with personal data these should be respected at all times:

* Right to respect for private and family life (Article 8).
* Freedom of thought, belief and religion (Article 9).
* Freedom of expression (Article 10).
* Freedom of assembly and association (Article 11).
* Protection from discrimination in respect of rights and freedoms under the HRA (Article 14).

**Complaints**

If you have a complaint or suggestion about the Company’s handling of personal data then please contact the person whose details are listed in the Appendix to this policy.

Alternatively, you can contact the ICO directly on: 0303 123 1113

or at: <https://ico.org.uk/global/contact-us/email/>

**Appendix**

Mr. Ian Shuttleworth (Director) & Mrs. Saran Cliff (Director) are responsible for:

1. adding, amending or deleting personal data;
2. responding to subject access requests/requests for rectification, erasure, restriction data portability, objection and automated decision-making processes and profiling;
3. reporting data breaches/dealing with complaints; and/or
4. details of the Data Protection Officer [where applicable].

**Annex**

1. The lawfulness of processing conditions for personal data are:
* Consent of the individual for one or more specific purposes.
* Processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual to enter into a contract.
* Processing is necessary for compliance with a legal obligation that the controller is subject to.
* Processing is necessary to protect the vital interests of the individual or another person.
* Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
* Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the individual which require protection of personal data, in particular where the individual is a child.
1. The lawfulness of processing conditions for sensitive personal data are:
* Explicit consent of the individual for one or more specified purposes, unless reliance on consent is prohibited by EU or Member State law.
* Processing is necessary for carrying out data controller’s obligations under employment, social security or social protection law, or a collective agreement, providing for appropriate safeguards for the fundamental rights and interests of the individual.
* Processing is necessary to protect the vital interests of the individual or another individual where the individual is physically or legally incapable of giving consent.
* In the course of its legitimate activities, processing is carried out with appropriate safeguards by a foundation, association or any other not-for-profit body, with a political, philosophical, religious or trade union aim and on condition that the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without the consent of the individual.
* Processing relates to personal data which are manifestly made public by the individual.
* Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
* Processing is necessary for reasons of substantial public interest on the basis of EU or Member State law which shall be proportionate to the aim pursued, respects the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the individual.
* Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or a contract with a health professional and subject to the necessary conditions and safeguards.
* 9. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the individual, in particular professional secrecy. 10. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard fundamental rights and interests of the individual.

Black Cat Recruitment Ltd is committed to the highest standards of professionalism and ethical operations when carrying out our recruitment and employment activities and are an active member of the Recruitment & Employment Confederation.

For more information on the REC, please visit:  www.rec.uk.com