DATA PROTECTION POLICY

Policy Statement

This Policy sets out how Carmichael[UK] (”we”, “our”, “us”, “the Company”) handle the Personal Data of our candidates, suppliers, employees, workers and other third parties.

This Policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, candidates, clients or supplier contacts, shareholders, website users or any other individual.

This Policy applies to all Company Personnel (”you”, “your”). You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements. This Policy sets out what we expect from you in order for the Company to comply with applicable law. Your compliance with this Policy is mandatory. Related policies and guidelines, such as our CCTV Policy, Privacy Policies and Data Retention Policy are available to help you interpret and act in accordance with this Policy. You must also comply with all such related policies and privacy guidelines. Any breach of this Policy may result in disciplinary action.

Carmichael[UK] is registered in the register of data controllers with the Information Commissioner’s Office (registration number Z8564246) and this registration is renewed on an annual basis.

For the purposes of understanding this policy the following words or phrases have the following meanings in accordance with current Data Protection law.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person’s actions or behaviour.

DATA PROTECTION POLICY

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

Policy Scope

We recognise that the correct and lawful treatment of Personal Data and Sensitive Personal Data will maintain confidence in the Company and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

All directors, officers and managers are responsible for ensuring all Company personnel comply with this Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The Managing Director is responsible for overseeing this Policy and, as applicable, developing related policies and guidelines. Please contact the Managing Director with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the Managing Director in the following circumstances:

- if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Company);
- if you need to rely on Consent and/or need Explicit Consent;
- if you are unsure about the retention period for the Personal Data being processed;

DATA PROTECTION POLICY

- if you are unsure about what security or other measures you need to implement to protect Personal Data;
- if there has been a Personal Data Breach;
- if you need any assistance dealing with any rights invoked by a Data Subject (see Section [12]);
- whenever you are engaging in a significant new, or change in, Processing activity or plan to use Personal Data for purposes others than what it was collected;
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties
- If you have need to or have been asked to transfer of information outside of the European Economic Area.

Policy Elements

Data Protection Principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

- processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
- collected only for specified, explicit and legitimate purposes (Purpose Limitation);
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
- accurate and where necessary kept up to date (Accuracy);
- not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
- not transferred to another country without appropriate safeguards being in place (Transfer Limitation);
- made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests)

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

DATA PROTECTION POLICY

Lawfulness, Fairness and Transparency

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

- the Data Subject has given his or her Consent;
- the Processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests;
- to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices; or

You must identify and document the legal ground being relied on for each Processing activity.

The GDPR requires that we provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them. The Company has in place Privacy Policies which comply with these obligations, one for staff and contractors and one for Candidates using our job finding services.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller, how and why we will use, Process, disclose, protect and retain that Personal Data by providing them with the appropriate privacy policy when the Data Subject first provides the Personal Data.

DATA PROTECTION POLICY

When Personal Data is collected indirectly (for example, from a third party or publicly available source), you must provide the Data Subject with the appropriate privacy policy as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

Consent

We must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, this must be captured in writing, with the written consent to be signed clearly and concisely explaining what Sensitive Personal Data we require, why we require it, how we will use it and explaining to the Data Subject that they have the right to withdraw their Explicit Consent at any time and how they can do this, also referring as necessary to the appropriate privacy policy and to the fact the Company is a Data Controller.

You will need to evidence Consent captured and keep records of all Consents so that the Company can demonstrate compliance with Consent requirements.

Accuracy of information, purpose limitation and data minimisation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

DATA PROTECTION POLICY

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted in accordance with the Company's data retention guidelines.

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Security, Integrity and Confidentiality

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

DATA PROTECTION POLICY

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.
You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

Data Protection Breaches

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches or the Operations Director. You should preserve all evidence relating to the potential Personal Data Breach.

Transfer of Personal Data to other Countries

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

DATA PROTECTION POLICY

You may only transfer Personal Data outside the EEA if one of the following conditions applies, and upon firstly obtaining prior approval from the Managing Director:

- the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;
- the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or
- the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

Use of Cookies & Similar Technologies

Cookies are small text files that are placed on a computer by websites visited. 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. The list below explains examples of cookies we may use and why.

Google Analytics - these cookies are used to collect information about how visitors use our site. We use the information to compile reports and to help us improve the site. The cookies collect information in an anonymous form, including the number of visitors to the site, where visitors have come to the site from and the pages they visited, including:

- Remembering choices, settings and preferences you made, so you do not have to keep re-entering them (functionality cookies);
- Remembering terms of use you have accepted so you do not need to keep accepting them (strictly necessary cookies). Without these cookies, information you are looking for cannot be provided;
- Measuring how you use the website so we can make sure it meets your needs (performance cookies).

Most web browsers allow people to modify preferences to notify them when a cookie is set, or to reject all cookies. Restricting or rejecting cookies on our website will mean that certain areas of the site will not function correctly.

DATA PROTECTION POLICY

Most web browsers allow some control of most cookies through the browser settings. The Company has provided information about cookies (including how to manage and delete them and to opt out of being tracked by Google Analytics) in its Cookie Policy on the top of each page of its website.

Data Subject Rights & Requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to Processing at any time;
- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on Automated Processing, including profiling (ADM);
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

Any requests received from a Data Subject to exercise any of the above rights should be made in writing and must be immediately passed onto the Operations Director who will, if considered appropriate, firstly verify the identity of an individual requesting data under any of the rights listed above before responding to the request. Do not allow third parties to persuade you into disclosing Personal Data without proper authorisation.

It is important such requests are passed onto the appropriate department to handle immediately on receipt as the Company shall have a maximum period of one month within which to respond.

DATA PROTECTION POLICY

In the case of receipt of a subject access request the following information will be provided to the data subject by the appropriate department:

- Whether or not the Company holds any personal data on the data subject;
- A description of any personal data held on the data subject;
- Details of what that personal data is used for;
- Details of any third-party organisations that personal data is passed to; and
- Details of any technical terminology or codes.

Record Management

Our records management procedure is designed to ensure that each record is managed through its life cycle from creation or receipt through maintenance and use to disposal or deletion. We focus on:

- Creating appropriate records and maintaining these on our system.
- Updating the information provided to us accurately.
- Reviewing the information held on a regular basis.
- Ensuring records are located correctly to enable ease of access and retrieval.
- Version control.
- Controlling the timescale and method for destruction of information.
- Managing information security to ensure personal, sensitive and confidential data is safe and secure from malicious access.

We define records as being documents, computer files, paper based files, email, diary records, faxes, reports and internet/intranet pages. All records pertaining to our clients, candidates and service are created and stored on our secure cloud based CRM system. This includes email communication, records of telephone conversations, scanned documents and information about candidates, clients, vacancies and search assignments, CV submissions, longlists, shortlists, placements and client/candidate feedback and diaries.

We retain a full inventory of records and communication relating to candidates, search assignments and clients on our system and such records can be viewed, updated, shared and deleted as appropriate by authorised personnel. Each member of our staff has their own individual login to the system and every action is time and date stamped together with the identity of the employee making the change or undertaking the action, giving a full audit trail which can be searched by client, candidate, search assignment or Carmichael[UK] employee.

Records can be received in hard copy or electronically and will be scanned and uploaded or saved against the relevant candidate, client or vacancy.

DATA PROTECTION POLICY

As part of induction, all staff are trained to use our systems and how to create, capture and input relevant information for the records that they have responsibility for to enable client, candidate, assignment and business information to be held in a consistent format and searched easily. They are also trained on how to dispose of paper records (using the confidential shredding facility) and delete electronic records.

Disposal of Records

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the Company's guidelines on Data Retention.

You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

You will ensure Data Subjects are informed of the period for which data is stored and how that period is determined by providing them with a copy of or directing them to the applicable Privacy Policy.

Electronic records will be deleted as appropriate, and we have facilities for the secure disposal of documentation relating to candidates, employees and clients.

Accountability

Carmichael[UK] as a Data Controller will, through appropriate management and the use of strict criteria and controls along with the strict observance of this and related policies by its staff:

- fully observe conditions regarding the lawful, fair and transparent collection and use of personal information;
- meet its legal obligations to specify the purpose for which information is used;

DATA PROTECTION POLICY

- collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- take appropriate technical and organisational security measures to safeguard personal information;
- ensure that personal information is not transferred abroad without suitable safeguards;
- ensure that the rights of people about whom the information is held and outlined above can be fully exercised under applicable Data Protection law.

In addition, Carmichael[UK] will ensure that:

- There is someone with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriately supervised.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All employees will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment.
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically.
- Individual passwords should be such that they are not easily compromised.
- Staff are required to sign a confidentiality agreement to protect both Carmichael[UK] and client sensitive/confidential data as part of their contract of employment.

All sub-contractors who are users of personal information supplied by Carmichael[UK] will be required to confirm that they will abide by the requirements of Data Protection Law with regard to information supplied by the Company.

DATA PROTECTION POLICY

We will collect relevant personal data from applicants / candidates in order to facilitate the recruitment process, further details of which can be found within the appropriate Privacy Policy. We will, where appropriate, obtain consent to use the personal data provided to facilitate the recruitment process on the applicant's or candidate's behalf and in accordance with the terms of this Data Protection Policy, the appropriate Privacy Policy and Data Protection law. We may also be given access to sensitive/confidential information to assist with fulfilment of recruitment projects and search assignments (e.g. organisational and business change strategies) and we will abide by our documented process in relation to creation, sharing, storage, processing and destruction of such data.

We will only allow access to applicant / candidate personal data by its staff and any prospective employers or clients for the purposes outlined within the applicable Privacy Policy and in accordance with this Policy.

We may be required to disclose personal data by law in connection with the detection of crime, the collection of taxes or duties, in order to comply with any applicable law, by order of a court of competent jurisdiction, or in connection with legal proceedings. However, prior approval of the Operations Director must be secured before disclosing any personal data on these grounds. We are required by law to hold applicant / candidate personal data for as long as is necessary to comply with our statutory and contractual obligations. The lawful grounds we rely on to hold and process an individual's personal data is explained within the relevant Privacy Policy and should be referred to as necessary.

Carmichael[UK] will use reasonable endeavours to ensure that personal data is maintained and up to date; however, applicants / candidates must be made aware they are under a duty to inform us of any and all changes to their personal data to ensure that it is up to date and we will update or delete their personal data accordingly. If we have no contact with the applicant / candidate then following the expiry of such reasonable period as we consider appropriate we will archive or, if appropriate, delete their personal information. If we consider it appropriate we may contact the applicant / candidate first and ask if they wish for their personal data to be maintained on our database or removed.

Applicant / candidate personal data is held on secure servers. The nature of the Internet is such that we cannot guarantee or warrant the security of any information transmitted via the Internet from applicants / candidates to us or from us to prospective Employers or Clients. No data transmission over the Internet can be guaranteed to be 100% secure; however, Carmichael[UK] will take all reasonable steps (including appropriate technical and organisational measures) to protect all personal data. Confidential and sensitive data in hard copy is held in locked filing cabinets with authorised keyholders.

DATA PROTECTION POLICY

Training and Audit

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

Sharing Personal Information

Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place, and the possibility of such data sharing is explained within the relevant privacy policy.

You may only share the Personal Data we hold with another employee, agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions and our publicised privacy policies.

You may only share the Personal Data we hold with third parties, such as our service providers if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Policy provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with Data Protection Law and has in place the required data security standards, policies and procedures and adequate security measures in place;
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains GDPR approved third party clauses has been obtained.

DATA PROTECTION POLICY

Conduct of Employment Agencies and Employment Businesses Regulations 2003

In line with the "Conduct Regulations" Carmichael[UK] will store candidate and client data for:

- At seven years after its creation (unless the data is in respect of applications which Carmichael[UK] takes no action); and
- At seven years after the date on which we last provide services to the associated applicant or client.

We may hold data significantly longer if contractually required and for contract clients, we will hold all data relating to service provided for a minimum of seven years after the contract expires. Where such records could be relevant to a claim for personal injury, we will retain them for a minimum of 21 years from contract expiry.

All data is stored securely on our electronic systems which are password protected. Where an employee leaves the business, their passwords and computer access is closed down immediately. We obtain and store the following information from candidates:

- Date the application was received.
- The candidate's name, address and date of birth.
- Any terms which apply or will apply between Carmichael[UK] and the candidate, and any document recording any variation thereto.
- Details of the candidate's training, experience, qualifications, and any authorisation to undertake particular work (and copies of any documentary evidence of the same).
- Details of any requirements specified by the candidate in relation to taking up employment.
- Names of clients to whom the candidate is introduced or supplied.
- Details of any resulting engagement and date from which it takes effect.
- Date the application was withdrawn or contract terminated (where applicable).
- Details about the candidate and the position concerned with copies of all relevant documents and dates they were received or sent as the case may be. These include:
    - The ID of the candidate.
    - The experience, training, qualifications and professional registrations.
    - References.
    - Confirmation that the candidate is willing to work in the position that they are being submitted for.
    - All relevant pre-employment checks.
    - Any information received by Carmichael[UK] to indicate that the candidate is unsuitable for the work being provided.

DATA PROTECTION POLICY

We obtain and store the following information about clients as a minimum:

- The date that the vacancy was submitted.
- The client's name, address and location of employment.
- Position(s) to be filled & job descriptions (which we may be instrumental in developing).
- Details of the client's organisational, financial and change strategies where they are appropriate to the role.
- Duration of assignment for interim or contract roles.
- Experience, training, ability, qualifications, professional memberships etc required in respect of the position(s) to be filled.
- Terms & conditions between the client and the agency.
- Name of candidates supplied or introduced.
- Details of assignment dates or placement start dates.
- Details of fees, pricing and payment including copies of statements and invoices.

Freedom of Information Act

Carmichael[UK]'s aim is to operate openly and honestly and in the interests of the public and with proper respect for its clients, employees and candidates.

To achieve this, we will:

- inform the requester if it holds the information specified in the request;
- provide the information to the requester or in the event of a refusal, inform the requester of the reason for the refusal;
- provide the information or a refusal within the timescales detailed below.

Any request made to Carmichael[UK] in writing in relation to a public function (including those transmitted by electronic means), stating the name of the requester, including an address for correspondence and describing the information required qualifies as a request for information.

We will inform the requester if we hold the information requested and if held (assuming the information requested does not fall into any of the exemption categories listed below) we will provide the information within 20 working days of receipt of the request. If the information requested does fall within the exemptions listed below, we will issue a Refusal Notice within 20 working days of the original request.

Any request for information under this policy should be made to the Managing Director and any member of staff receiving such a request should forward it to this person immediately.

DATA PROTECTION POLICY

In some circumstances a request may be refused. The Act recognises that there are valid reasons for withholding information examples of which include:

- Where the information is reasonably accessible to the applicant by other means.
- Where the information has been supplied by one of the specified security bodies or it is in the interests of national security not to disclose it.
- Where the information is a trade secret or was provided in confidence.
- That is vexatious or repeated (i.e. where the request is likely to cause distress, disruption or irritation without any proper or justified cause).
- That relates to accessing the requester's personal information as this relates to data protection legislation and the process for making such a request is covered elsewhere in this policy.
- Where the release of the information is likely to prejudice the commercial interests of any person, company, authority or third party. This will include:
    - details of clients or candidates;
    - details of the company's contracts;
    - pricing and any other commercially sensitive information relating to the company and its clients;
    - financial information that could expose the company, its clients, candidates or Service Users to fraud;
    - the company's future business strategy;
    - the company's IT Security and Business Continuity strategies.
- Where the information would be likely to endanger the physical or mental health or safety of any individual.
- Where it would be illegal to disclose the information.

Implementation

The Operations Director will be responsible for ensuring that the Policy is implemented. Implementation will be led and monitored by the Operations Director who will have overall responsibility for:

- The provision of cascade data protection training, for staff within the company.
- For the development of best practice guidelines.
- For carrying out compliance checks to ensure adherence with the Data Protection Act.
- Ensuring all employees sign the company's confidentiality agreement and understand the penalties for deliberate misuse, damage, theft or destruction of records.

DATA PROTECTION POLICY

Responsibilities

It is the direct responsibility of the Operations Director to ensure the implementation of this policy on a day-to-day basis; however, all employees have a responsibility to accept their personal involvement in applying it and must be familiar with the policy and ensure that it is followed by both themselves and employees for whom they have a responsibility.

Disciplinary action may be taken against any employee who acts in breach of this policy. Disciplinary action may include summary dismissal in the case of a serious breach of this policy or repeated breaches. In other cases, it may include a warning, oral or written. Such action will be taken in accordance with the Company's disciplinary procedure.

Breaches of this policy may also result in the employee responsible being held personally liable for compensation if legal action is taken in relation to a Data Protection Breach.

Approval & Review

This privacy policy statement will be reviewed once a year to ensure continuing suitability with business requirements. As necessary additional alterations may be made from time to time in the light of legislative changes, operational procedures, or other prevailing circumstances.

This policy statement has been approved by the Board of Directors to ensure it is fit for the purposes of the business in connection with processing of individual's data.