Privacy Statement

WELCOME TO CORE-ASSET CONSULTING

Privacy statement

At Core-Asset, we are committed to protecting and respecting your privacy.

This statement explains when and why we collect personal information about people who engage with our services, how we use it, the conditions under which we may disclose it to others, and how we keep it secure.

It covers our employees, candidates, temporary workers and contractors, client and supplier contacts, referees and emergency contacts, and visitors to our office and website.

We may update this statement from time to time. If we make significant changes, we will tell you directly where we hold your contact details, as well as publishing the updated version on our website.

This statement applies when you engage with us, for example by applying for a job we are advertising, registering through our website or getting in touch with our business. It is not a contract, and engaging with us does not by itself mean that you have consented to anything. The lawful bases on which we rely are explained in the section 'Legal basis to process your data' below.

Any questions regarding this statement and our privacy practices should be sent by email to our Data Protection Lead, Julie Fraser – julie@core-asset.co.uk – or by writing to Julie Fraser, 37 Melville Street, Edinburgh, EH3 7JF.

Who are we?

We are Core-Asset Consulting, a recruitment business dedicated to finding people jobs in the professional and financial services, accounting & legal sectors within Scotland and the UK.

Core-Asset Consulting Limited is a private limited company registered in Scotland (company number SC282072), with its registered office at 37 Melville Street, Edinburgh, EH3 7JF. We are the controller of the personal information described in this statement, and we are registered with the Information Commission (formerly the Information Commissioner's Office) under registration number Z1075824.

How do we collect information from you?

We obtain information about you when you engage with us. For example:

- When you apply for a job we are advertising either on our own website or on our partners' job-board websites;
- When you register on our website or enquire about our services;
- When you meet with us in person and complete our registration forms;
- When you secure a role, as we may need to collect extra information from you to carry out background checks using our electronic vetting forms;
- When you complete our surveys, as from time to time we may ask you how we can improve our services.

We also receive information about you from other sources, including:

- job boards and CV databases where you have posted your CV (for example, Indeed, Adzuna, etc.);
- professional networking sites such as LinkedIn, where you have made your profile publicly available;
- people who recommend you to us, and referees you nominate;
- our clients, for example interview feedback; and
- background screening and identity verification providers, where checks are carried out (see below).

Where we obtain your information from someone other than you, we will tell you within one month and point you to this statement.

What type of information do we collect from you?

The personal information we collect from you commonly includes the type of information that is likely to be listed on your CV, for example, your name, address, contact information, educational and work history.

We are likely to ask you for additional details to help you find a job and comply with our legal obligations. For example, the type of job you are looking for, your salary expectations, your nationality, and your ability to work in the UK (for which you will be asked to provide documentary evidence).

We may also invite you to provide equality monitoring information, such as your age, sex or gender, ethnicity, religion or belief, sexual orientation and any disability. Some of this is 'special category' data, which the law protects more strictly.

The reason we ask for this sort of data is to assist us in monitoring our diversity and inclusion statistics. This information is not used in any other way. It is stored separately from your candidate record, reported only in aggregate form, and never shared with our clients or used in decisions about you. Also, it is entirely optional if you wish to share this information with us and by doing so help us promote diversity and inclusion across our services.

If we are engaging with you to perform pre-employment background checks, it is likely we will need to ask you for additional personal information to carry out this service.

This is likely to include your financial history, criminal record information, referee details and verification of your qualifications. We will explain the checks needed for the role and ask for your authorisation before any check is carried out. The lawful bases we rely on are set out in 'Legal basis to process your data' below.

If we are engaging with you because we are acting as your employment business (for example, where you are temping or contracting through us), it is likely we will ask for additional information to provide these services and meet our legal obligations.

This will be information such as your bank details (so we can pay you), your tax and National Insurance details, your next of kin's contact details (in the event of an emergency) and any reasonable adjustments you may require from your workplace (for example, as a result of a disability).

If you have engaged with us via our website, it is likely we will have retained additional information that is not listed above (such as your IP address and browsing habits). Please see section 'use of cookies' for more information.

How is your information used?

We may use your information to:

- help you find a job by notifying you of new vacancies;
- share with our clients to help you find a job (we will always discuss a role with you and get your agreement before sending your details to a client);
- send you communications in relation to your job search and our recruitment services;
- send you communications in relation to hiring new talent (our clients only);
- carry out our obligations arising from any contracts entered into by you and us;
- seek your views or comments on the services we provide;
- notify you of changes to our services to you;
- perform pre-employment background checks (where required for a role you have accepted);

- act as your employment business if you are temping or contracting through us, including paying you and meeting our legal obligations;
- record and summarise calls (see 'Call recordings' below);
- comply with our legal and regulatory obligations;
- establish, exercise or defend legal claims.

We keep personal information only for as long as we need it. Due to the long-term nature of job searching and the relationship with our clients, our standard retention period for candidate and client contact records is five years from our last meaningful contact with you. Some information is kept for a shorter or longer period:

- applications for a specific role made through a job board that do not progress, where you have not otherwise registered with us: six months from the date of your application. These applications are held in Veritone Hire (Broadbean) and are not added to our candidate database;
- identity and right to work documents: for the duration of any assignment plus two years;
- background checks carried out by Core-Asset Verify: verification reports and right to work checks are kept for five years, unless the client asks for a shorter period; DBS certificate information is kept for no longer than six months after the recruitment decision, unless a dispute or complaint is raised; and supporting documents are deleted once the check is complete;
- payroll, tax and pension records for temporary workers and contractors: six years from the end of the tax year to which they relate;
- call recordings: three months (see 'Call recordings' below).

At the end of the relevant period, we securely delete or anonymise the information.

Who has access to your information?

We will not sell or rent your information to third parties.

We will not share your information with third parties for marketing purposes.

Our clients

To find you a job, it perhaps comes as no surprise that we need to share your details with our clients, who may ultimately go on to be your future employer. This may involve uploading your data onto our clients' websites, recruitment systems or sharing via email.

We will always discuss a role with you and get your agreement before sending your CV or details to a client, and we keep a record of this. Our clients may choose to contact you directly following this, to request additional information and share their own privacy policy with you.

Third-party product providers

We use service providers that process personal information on our behalf (known as 'processors').

They provide services such as our email system, candidate database, electronic forms, telephony, identity verification, website and finance systems. They act only on our instructions, under written contracts that require them to keep your information secure, and they may not use it for their own purposes. Our main processors, and where they process your information, are listed in the table under 'Transferring your information outside of the UK' below.

When you apply for a role through a job board or our website, your application is received and managed through Veritone Hire (Broadbean), which also sends some emails to you on our behalf, for example to let you know that an application will not proceed. Broadbean records whether these emails are delivered, and uses unique application links to record which advert or job board an application came from. It does not use tracking pixels to record whether you open our emails.

Core-Asset carries out regular risk assessments of our third parties and monitors the effectiveness of the security protections they provide.

Where necessary, we may also share your information with other organisations, including HMRC and other public authorities, pension providers, payroll or umbrella companies (for temporary workers and contractors), our insurers, auditors, certification bodies and professional advisers.

We may transfer your personal information to a third party:

- as part of a sale of some or all of our business and assets to any third party;
- as part of any business restructuring or reorganisation;
- if we are under a duty to disclose or share your personal data in order to comply with any legal obligation;
- to enforce or apply our terms of use;
- to protect the rights, property or safety of our candidates, clients, staff or others.

However, we will take steps to ensure your privacy rights continue to be protected.

In the event we are performing pre-employment background checks, it is likely we will be sharing your data with additional third-party providers such as credit agencies, criminal record agencies (such as Amiqus, uCheck and Disclosure Scotland), international screening providers (Owens), media search providers (SP Index), your previous employers, and educational establishments.

In these cases, we will explain the checks before they take place and ask you to complete an authorisation form.

Your choices

You have a choice whether you wish to receive information from us and continue to use our services. If you do not want to receive communications from us about our recruitment services, you can ask us at any time to stop contacting you or to delete your information.

You have the following rights over your personal information:

- **Access** – to ask for a copy of the information we hold about you (a 'subject access request').
- **Rectification** – to ask us to correct inaccurate or incomplete information.
- **Erasure** – to ask us to delete your information (sometimes called 'the right to be forgotten'). This right is not absolute: we may need to keep some information, for example to meet a legal obligation.
- **Restriction** – to ask us to limit how we use your information in certain circumstances.
- **Objection** – to object to processing based on our legitimate interests, and to object at any time to direct marketing.
- **Portability** – to receive information you have given us in a structured, machine-readable format, where our processing is based on your consent or a contract and is carried out by automated means.
- **Withdrawing consent** – where we rely on your consent, to withdraw it at any time. This does not affect processing carried out before you withdraw it.
- **Automated decisions** – to be told about, make representations about, obtain human review of and challenge significant decisions made solely by automated means (see 'Profiling and Automated Decisions' below).

We will respond to a subject access request within one calendar month of receipt. If your request is complex or you have made a number of requests, we may extend this by up to two further months; if so, we will tell you within the first month and explain why. If we need further information from you, for example to confirm your identity or clarify your request, the time limit may be

paused until we receive it. We will carry out reasonable and proportionate searches for your information.

You can make a request in any way, including verbally, but it helps us if you email our Data Protection Lead, Julie Fraser, at julie@core-asset.co.uk or by writing to us at Julie Fraser, Core-Asset Consulting, 37 Melville Street, Edinburgh, EH3 7JF. It also helps if you mark your correspondence with the right you are exercising, for example 'Subject Access Request' or 'Right to be Forgotten'.

Where we send job alerts to candidates, or information about our services to client contacts, we do so in line with the Privacy and Electronic Communications Regulations (PECR). You can opt out at any time by using the unsubscribe link in our emails or by contacting us. We will not share your information with third parties for their own marketing.

How you can update your information

The accuracy of your information is important to us.

If any of your information changes, or any of the information we hold is inaccurate or out of date, please email us at recruitment@core-asset.co.uk or write to Core-Asset Consulting at 37 Melville Street, Edinburgh, EH3 7JF. Alternatively, please contact your consultant at Core-Asset.

Processing of your personal data under the UK General Data Protection Regulation (UK GDPR)

As a recruitment business offering a wide range of services, we process personal data in relation to our staff, candidates, suppliers, and client contacts. It is crucial that we abide by the principles of UK GDPR as set out below.

Our purposes for processing personal data

We process your data for the following purposes:

- For **our candidates**, to provide job finding services;
- For **our contractors**, to comply with all industry and employment regulations and meet all our obligations as an employer;
- For **our clients**, to assist with finding suitable candidates and meet our contractual obligations;
- For **our suppliers and partners**, to meet our respective contractual obligations.

Principles relating to the processing of personal data under UK GDPR

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be 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
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the UK GDPR

For more information about how we abide by each principle, please request our Data & Information Security policy document by contacting our Data Protection Lead, Julie Fraser, at julie@core-asset.co.uk.

Legal basis to process your data

We rely on the following lawful bases under Article 6 of the UK GDPR:

- **Legitimate interests** – to provide our recruitment services, including registering you, assessing applications you make through our website or job boards, matching you to roles, sharing your details with clients (with your agreement), keeping in touch about suitable opportunities, managing client and supplier relationships, recording and summarising calls, and improving our services. Our legitimate interests, and those of our clients, are finding suitable candidates for roles and helping candidates find work. You have the right to object to this processing at any time.
- **Contract** – where processing is necessary to enter into or perform a contract with you, for example your assignment terms as a temporary worker or contractor, or our terms of business with clients and suppliers.
- **Legal obligation** – where the law requires us to process information, for example right to work checks, PAYE and National Insurance, pension auto-enrolment, and record-keeping under the Conduct of Employment Agencies and Employment Businesses Regulations 2003.
- **Consent** – only where we specifically ask for it, for example where you choose to provide optional equality monitoring information. You can withdraw your consent at any time by contacting us.

Special category and criminal offence data

Where we process special category data (such as health or disability information, or equality monitoring data) or criminal offence data, we also rely on an additional condition under Article 9 or Article 10 of the UK GDPR and Schedule 1 of the Data Protection Act 2018. These include:

- employment and social security law, for example to make reasonable adjustments for temporary workers and contractors;
- equality of opportunity or treatment, for optional equality monitoring;
- regulatory requirements relating to unlawful acts and dishonesty, for criminal record and financial probity checks required for roles in regulated financial services; and
- your explicit consent, where no other condition applies.

Providing your information

You are not legally required to give us your information. However, if you do not provide the information we need, for example your contact details, right to work evidence or the information needed for background checks required by a client, we may not be able to put you forward for roles or engage you on an assignment.

Security precautions in place to protect the loss, misuse or alteration of your information

When you give us personal information, we take steps to ensure that it is treated securely.

We use appropriate technical and organisational measures to protect your information, including encryption, access controls and multi-factor authentication. We hold ISO 27001 (information security) and ISO 22301 (business continuity) certifications.

Once we receive your information, we make our best effort to ensure its security on our systems – a more detailed description of

our security controls can be found in our Data & Information Security policy document, which is available upon request by contacting our Data Protection Lead, Julie Fraser, at julie@core-asset.co.uk.

Profiling and Automated Decisions

Profiling and automated decision-making tools do **not** form part of our services, except some elements of our pre-employment vetting services (such as a financial probity check). Where a check involves a decision based solely on automated processing that has a legal or similarly significant effect on you, we will tell you before the check takes place. You can make representations about the decision, ask for a member of our team to review it, and challenge the outcome.

Note: Profiling is (a) the automated processing of personal data; and (b) using that personal data to evaluate certain personal aspects relating to a natural person. Specific examples include analysing or predicting "aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

We do use automation in our database in order to shortlist candidates, but the automation only looks at limited data such as job title and location. It does not screen out candidates but adds registered candidates to existing shortlists. All applications and shortlisted candidates are reviewed by our consultants. Decisions not to progress an application are always made by a consultant, even where the notification is sent automatically through Veritone Hire (Broadbean).

Use of Artificial Intelligence (AI) tools

Nature and purpose of our AI tools

We use AI-assisted search and matching (Bullhorn auto-match and LinkedIn AI-Assisted Search) to help us find candidates, but we do not use AI tools to screen or select candidates, and all decisions about candidates are made by people. Where our AI tools process your personal information, it is not used to train their models.

We use generative AI features in some of our tools, including our VoIP call system (Devyce), Claude (including AI agents provided by Soria Labs), Microsoft Copilot and Read AI (for notes of client meetings). Their purpose is to improve our operational efficiency, and approved uses are limited to generating meeting notes and call summaries and assisting with administrative tasks such as writing job adverts, formatting CVs and preparing verification reports for background checks. This means your personal information, such as your CV, the results of background checks or what you discuss with us on a call, may be processed by these tools. We use Claude under a business licence and Microsoft Copilot through our Microsoft 365 work accounts, both covered by data processing agreements. We also use other AI tools, such as ChatGPT, Grammarly and Perplexity, for general drafting and research, but we do not enter your personal information into them.

A member of our team reviews all AI-generated content before it is used or shared. We rely on our legitimate interests for this processing, and we have assessed the risks in a data protection impact assessment and / or an AI Risk Assessment.

UK White Paper: A pro-innovation approach to AI regulation

The UK Government's White Paper, A pro-innovation approach to AI regulation, sets out five non-statutory principles. We follow them alongside our obligations under data protection and equality law:

Safety, security and robustness	We follow cybersecurity and data privacy best practices, and we hold ISO 27001 and 22301 certifications.
Appropriate transparency and explainability	We provide information about the nature, purpose and outcome of our use of AI in our Privacy Statement (this document)
Fairness	We use AI-assisted search to help find candidates, but we do not use AI to screen or select them, and decisions about candidates are always made by people. We are committed to treating everyone fairly and without bias or discrimination, and we review AI-generated content, such as job adverts and formatted CVs, for accuracy and bias before it is used.
Accountability and governance	Our AI framework and policy are reviewed and assessed regularly, and any identified gap is discussed and actioned by Senior Management.
Contestability and redress	You can address any concern or issue to our Data Protection Lead at julie@core-asset.co.uk.

Call Recordings

Our calls are recorded for quality and training purposes, and to produce AI-generated call summaries (see 'Use of Artificial Intelligence (AI) tools' above). We rely on our legitimate interests for this, and we tell callers at the start of each call that it is being recorded. Recordings are stored on our VoIP supplier's platform for three months and then deleted.

You can ask us not to record a call, or object to us keeping a recording, and we will consider your request in line with your right to object.

Visiting our office

Our office at 37 Melville Street is covered by cameras operated by our landlord, MS37 Ltd, for the security of the building. If you visit us, we will ask you to sign our visitor log, which we keep for two weeks. If we need to investigate an incident, we may obtain a copy of relevant footage from MS37 Ltd, which we keep only until the investigation, and any resulting action, has concluded.

Requests to see footage held by MS37 Ltd should be made to them directly.

Use of 'cookies'

Like many others, Core-Asset Consulting's website uses cookies. 'Cookies' are small files placed on your device that allow a website to recognise your device when you visit.

They collect statistical data about your browsing actions and patterns. For example, we use cookies to store your browsing preferences. This helps us to improve our website and deliver a better and more personalised service.

We set non-essential cookies, including Google Analytics, only after you have given your consent through the cookie banner on our website. If you want to change your choice, you can clear our cookies in your browser settings, and the banner will appear again on your next visit.

We currently use the following cookies on our website:

- **Google Analytics** (_ga, _gat, and _gid): used, with your consent, to collect statistics about how visitors use our website. These cookies last up to two years.
- **Cookie consent** (CookieControl): a strictly necessary cookie that remembers whether you have accepted or rejected cookies, so that we do not ask you again on every visit. It lasts 90 days.

We are launching a new website and will publish a full cookie policy alongside it, setting out each cookie we use, its purpose and how long it lasts. We will link to it from this statement once it is available.

It is possible to switch off cookies by setting your browser preferences. Please note that turning cookies off may result in a loss of functionality when using our website.

Cookie identifiers and IP addresses can be personal data, and we treat them as such.

Transferring your information outside of the UK

As part of our services, some of the information which you provide to us, on occasions, may be transferred to countries outside the United Kingdom (UK).

For example, this may be when we need to perform a pre-employment background check if you have lived and worked overseas, and we need to verify this. Where no other safeguard is available, we will rely on your explicit consent, and we will tell you about the possible risks of the transfer before asking for it.

When selecting software suppliers, we prefer vendors that store data within the UK, as this means your data remains protected by UK data protection law.

However, some of our providers, including our AI tools and website analytics, process data outside the UK, including in the European Union (EU) and the US.

If we transfer your information outside of the UK in this way, we will take steps to ensure that appropriate security measures are taken, with the aim of ensuring your privacy rights continue to be protected as outlined in this statement. In each case we rely on one of the safeguards set out in Chapter V of the UK GDPR: UK adequacy regulations (which cover, for example, countries in the European Economic Area), the UK Extension to the EU-US Data Privacy Framework for certified US providers, or the International Data Transfer Agreement or UK Addendum to the EU Standard Contractual Clauses. The providers concerned and the safeguard relied on for each are set out below.

Provider and purpose	Where data is processed	Safeguard
Bullhorn – candidate database and onboarding	UK	N/A – No transfer outside the UK.
Veritone Hire (Broadbean) – job advert distribution and applications	All data is stored and processed using servers located Ireland (Amazon Web Services). Support staff in the USA, Australia and India may access the data.	UK adequacy regulations (Ireland). For access by support staff outside the UK/EEA: EU Standard Contractual Clauses with the UK Addendum.
Microsoft – email, Teams and Copilot	Exchange, SharePoint, OneDrive, Teams and Copilot content in the UK.	Microsoft DPA, including SCCs with the UK Addendum and the UK Extension to the EU-US Data Privacy Framework.
Devyce – telephony and call recording	UK	N/A – No transfer outside the UK.
Anthropic – Claude (AI assistant)	US	Anthropic DPA, including SCCs with the UK Addendum.
Soria Labs – AI agents (using Claude) for CV formatting and verification reports	US	Anthropic DPA, including SCCs with the UK Addendum.
Read AI – notes of client meetings	Data is stored encrypted at rest on AWS in Northern Virginia	EU-US Data Privacy Framework
Amiqus – identity verification	UK	N/A – No transfer outside the UK.
uCheck – DBS checks	UK	N/A – No transfer outside the UK.
Owens – international criminal and financial checks	US	**Standard Contractual Clauses & UK Addendum.** For transfers originating from the UK, EEA, or Switzerland, Owens relies on the European Commission's **Standard Contractual Clauses (SCCs)** and the **UK International Data Transfer Addendum** (alongside adequacy decisions where applicable)
SP Index – online and adverse media searches	UK / EEA	UK International Data Transfer Agreements (IDTAs) or adequacy regulations
DocuSign – electronic signatures	UK accounts are provisioned into Docusign's Europe region (Frankfurt, Amsterdam, and Paris)	Docusign is one of the few SaaS vendors with EU-approved **Binding Corporate Rules (BCRs)** for both processors and controllers, alongside **EU Standard Contractual Clauses (SCCs)** and the **UK International Data Transfer Addendum**.
Website (Marketing Concept)	UK	N/A – No transfer outside the UK.
Google Analytics	Does not log or store full IP addresses. IPs are processed locally on regional servers only to derive geo-location metadata (such as city or country) and are then immediately discarded before data storage. Analytics data is processed by Google and may be stored on servers in the US.	Google's data processing terms, including the UK Extension to the EU-US Data Privacy Framework and SCCs with the UK Addendum
Xero – finance system	UK	N/A – No transfer outside the UK.

Provider and purpose	Where data is processed	Safeguard
Datto – backup of Microsoft 365 data	UK	N/A – No transfer outside the UK.
CharlieHR – HR and leave management (staff only)	UK	N/A – No transfer outside the UK.

If you use our services while you are outside the UK, your information may be transferred outside the UK to provide you with those services. In that case, the transfer is necessary to provide the services you have asked us for.

Information about our staff

This section applies to our own employees and workers, and to people who apply for roles at Core-Asset itself. It does not cover the temporary workers and contractors we place with clients, whose information is described elsewhere in this statement. The rest of this statement, including your rights and how to complain, also applies to you.

What information we hold

We hold the following information about you:

- your contact details, date of birth, and emergency contact and next of kin details;
- recruitment information, such as your CV, interview notes, references and right to work documents;
- your contract, job title, working hours, salary, commission, benefits and pension details;
- bank, tax and National Insurance details, so we can pay you;
- attendance and leave records, including holidays, sickness absence and family leave;
- performance and development information, such as appraisals, objectives and training records, and records of any disciplinary or grievance matters;
- information about your use of our IT systems, email and telephony, including call recordings and, where needed to investigate an incident, copies of CCTV footage (see 'Visiting our office');
- health information, such as fit notes, occupational health reports and details of reasonable adjustments; and
- optional equality monitoring information and the results of any pre-employment background checks.

Why we use it and our lawful bases

We use your information to recruit you and manage your employment, including paying you, managing performance, leave and absence, training and development, health and safety and IT security, and handling disciplinary matters, grievances and legal claims. We rely on the following lawful bases:

- **Contract** – to enter into and perform your employment contract, for example paying you and providing your benefits.
- **Legal obligation** – to meet our obligations under employment, tax, immigration and health and safety law, for example right to work checks, PAYE, statutory sick and family pay, pension auto-enrolment, and working time and minimum wage records.
- **Legitimate interests** – to run and protect our business, for example performance management, IT security and monitoring, call recording, business planning, and providing references when you ask us to. We have balanced these interests against your rights.
- **Consent** – only for optional matters, such as equality monitoring information. Because of the nature of the employment relationship, we do not rely on consent for anything you need to do as part of your job. You can withdraw your consent at any time.

We use health information to manage sickness absence, sick pay, occupational health and reasonable adjustments, relying on the employment and social security law condition in Schedule 1 of the Data Protection Act 2018. Equality monitoring information is used only for equality monitoring, as described above.

Who we share it with

Where necessary, we share your information with HMRC, our payroll provider (RSM), our pension provider (Royal London), CharlieHR (our HR and leave management system), the IT and software providers listed in the table under 'Transferring your information outside of the UK', occupational health advisers, our professional advisers and auditors, and certification bodies for our ISO audits. We will only provide a reference to a future employer if you ask us to.

Monitoring

We monitor the use of our IT systems, email and telephony to protect the security of our systems and the information we hold, to meet our ISO 27001 obligations, and to investigate suspected misuse. Any monitoring is proportionate, and further details are set out in our Access Control Policy.

How long we keep it

We keep your employment records for six years after your employment ends, which reflects the time limits for bringing legal claims. Some records are kept for a different period:

- payroll, tax and pension records: six years from the end of the tax year to which they relate;
- right to work documents: for the duration of your employment and two years afterwards;
- employment reference letter for former employees (including only name, job title and dates of employment): indefinitely;
- applications for roles at Core-Asset that do not progress: six months from the date of the decision;
- DBS certificate information: no longer than six months after the recruitment decision, unless a dispute or complaint is raised;
- call recordings: three months (see 'Call recordings' above).

Making a complaint

If you wish to complain about how we have handled your personal information, please contact our Data Protection Lead, Julie Fraser (julie@core-asset.co.uk). You can complain in writing, by email or by phone.

We will acknowledge your complaint within 30 days of receiving it, look into it without undue delay, and tell you the outcome, also without undue delay. We may ask you for further information to help us investigate.

You also have the right to complain to the Information Commission, which continues to operate as the Information Commissioner's Office (ICO), at any time. The ICO normally expects you to raise your concern with us first, so that we have a chance to put things right.

ICO helpline: 0303 123 1113

Website: ico.org.uk/make-a-complaint

Review of this statement

We keep this statement under regular review. It was last updated on **19 November 2026**.