

HR Privacy Notice

Employees, Temporary Workers and Contractors

Respect

Excellence

Attention

Challenge

Honesty

Contents

About us	3
Who this privacy notice applies to	3
Why we are providing you with this privacy notice	3
How we obtain your personal data	4
The types of personal data we will have about you	4
Personal data	4
Special category data	5
How we will use your data	6
Call recording	8
The legal grounds on which we will process your data	8
Who we share your data with	9
How long we will hold your data for	10
Credit reference agencies	10
Fraud prevention agencies	10
If you choose not to give us personal data	11
Your legal rights	11
Sending your personal data outside the United Kingdom and European Economic Area	11
How to complain	12

About us

Charter Court Financial Services is a trading name of Exact Mortgage Experts Limited which is part of the Charter Court Group. The Charter Court Group is made up of Charter Court Financial Services Group plc and its subsidiary companies Charter Court Financial Services Limited, Charter Mortgages Limited, Exact Mortgage Experts Limited and Broadlands Finance Limited.

Exact Mortgage Experts Limited will be a data controller of any personal data it holds about you and your application for or a role with and employment by or work with us. We may share this information with other parts of the Charter Court Group. Where this occurs, they will be a separate data controller in respect of that personal data, and this privacy notice will also apply to any processing they undertake, unless they provide you with an alternative privacy notice.

A data controller is an individual or organisation which decides how your personal data will be used. The data controller is referred to as "we", "us" and "our" in this privacy notice.

If you require any further information or wish to contact us or our Data Protection Officer at any time our contact details are:

Address: Charter Court Financial Services
2 Charter Court
Broadlands
Wolverhampton
WV10 6TD

Telephone Number: 0333 014 3477

DPO Email: thedataprotectionofficer@chartercourtfsc.co.uk

Who this privacy notice applies to

This privacy notice explains how we will use the personal data of potential, current and previous:

- employees;
- temporary workers;
- contractors, and
- directors.

Each such person is referred to as "you" and "your" in this privacy notice.

Why we are providing you with this privacy notice

Applicable Data Protection laws (including the General Data Protection Regulation 2016 and the Data Protection Act 2018), impose obligations on us as the data controller, when we collect or create, hold, amend, disclose, share or otherwise use or erase/destroy (collectively referred to as processing) your personal data and give you, as the data subject, rights over your personal data.

One such obligation is to process, (e.g. collect, hold, use or erase) your personal data, fairly, lawfully and in a transparent manner. This privacy notice meets that obligation by explaining what personal data we will hold about you, how we will process your personal data, why we process your personal data and the lawful grounds on which we are processing it. It also sets out some of your legal rights.

We may change this privacy notice in the future. If we make any substantial and/or material changes and those changes materially affect you, we will inform you of any changes before they take effect.

This privacy notice does not form part of any contract of employment or other contract to provide services.

How we obtain your personal data

We will mainly receive personal data about you from you, either directly or through an employment agency. This will be from application forms, CVs, identity documents (e.g. your passport and driving licence), forms completed by you at the start of and during your employment or engagement, correspondence with you, through interviews, meetings or other assessments.

We will also receive data from other sources including:

- persons who represent or advise you;
- employment agencies and former employment agencies;
- former employers;
- credit reference agencies;
- fraud prevention agencies;
- Higher Education Degree Check (HEDD);
- our regulators including the Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA);
- your mortgage lender or landlord for references;
- your bank or building society;
- GPs, consultants, occupational health and counselling providers;
- our auditors, accountants, and solicitors;
- companies providing training to you or accreditors of training we offer;
- companies which provide the benefits we offer including pension, childcare vouchers, SAYE, Share Incentive Plan, employee incentive plans, life assurance, private medical and dental insurance, group income protection, group critical illness, car insurance (where applicable for role);
- persons working on our behalf and providing us services;
- local and national government including the Department for Work and Pensions, Her Majesty's Courts Service, Child Support Agency, the Disclosure and Barring Service, the Office of National Statistics, Job Centre Plus;
- tax and law enforcement agencies;
- market research companies, and
- other companies within the Charter Court Group.

We may also obtain data about you that is publicly available, such as from the Electoral Register, Companies House and the internet

The types of personal data we will have about you

Personal data

We may process a wide variety of data about you, where necessary, for the purposes set out in the "How We Will Use Your Data" section, including data about:

you as an individual	<ul style="list-style-type: none"> • name, title and address (including previous names and addresses and date of change) • other contact details including email addresses and telephone numbers • gender, date of birth, place of birth and marital status including date of marriage or civil partnership • expected retirement age • nationality • national insurance number • details of any different languages you speak • tax code and tax information • your image in CCTV and photographs • use of our information and communications systems • entry to and from our premises
----------------------	--

your employment or engagement and previous employment or work	<ul style="list-style-type: none"> • payroll number • passwords • regulatory reference numbers • employment or work history with us and previous employers including employment status, length of employment or engagement (start and end dates), reason for leaving and any termination payments • the terms and conditions of your employment or your engagement • pay and benefits including allowances, deductions, statutory leave and pay from a previous employer in the tax year of your employment by us • your pension(s) • your entitlement to and participation in benefits we offer • any other employment or engagement you have during the course of your employment or work with us including companies of which you are a director and partnerships in which you are a partner • student loans • attachment of earnings orders • whether you have ever been disqualified as a director or subject to any regulatory investigation or censure
people connected to you	<ul style="list-style-type: none"> • next of kin (name, address, telephone number and relationship with you) • emergency contact details (name, address, telephone number and their relationship with you) • beneficiary details (name, address, date of birth, telephone number and their relationship with you).
your bank information	<ul style="list-style-type: none"> • bank details (sort code, bank account number and name of account holder)
your right to work in the UK	<ul style="list-style-type: none"> • passport number, visa, residence permit or birth certificate
your credit history and any criminal record	<ul style="list-style-type: none"> • credit history • criminal record • fraud
your working pattern and leave	<ul style="list-style-type: none"> • days and hours of work; • periods of, and reasons for, absence including for holiday, sickness and family leave
your performance at work	<ul style="list-style-type: none"> • assessments of your performance, including performance reviews and ratings, targets and objectives, notes of performance rating appeal hearings, performance improvement plans and related correspondence • continuous professional development, courses and training you have undertaken
disciplinary, grievance, absence and performance management	<ul style="list-style-type: none"> • details of any disciplinary, grievance, absence management or performance management procedures in which you have been involved, including records of meetings and investigations, data about any warnings issued to you, notifications to any regulator and related correspondence
your correspondence and documents we hold	<ul style="list-style-type: none"> • documents we hold (e.g. driving licence, passport, birth certificate) correspondence or communications received or sent and the information contained within them
your car and driving record	<ul style="list-style-type: none"> • number plate registration, make and model • driving licence details (including endorsements and disqualifications, where applicable).

Special category data

Some personal data for example data about your health, racial or ethnic origin is subject to additional rights and are described as special category data. The special category data which we may have about you is:

medical data	<ul style="list-style-type: none"> • medical or health conditions • disability data to enable us to make reasonable adjustments • work-related injury and illness • lifestyle information • spouse/dependants medical or health conditions
equal opportunities monitoring data	<ul style="list-style-type: none"> • your ethnic origin, sexual orientation, health and religion or belief
employee representation and trade union data	<ul style="list-style-type: none"> • your representative details • your case details • your membership details

We will only process special category data if you have confirmed your consent to us doing so, or where we are legally permitted or required to process this information without seeking your consent. Where we have obtained your consent to us processing special category data in this way, you are entitled to withdraw your consent to this at any time. Please contact us if you wish to do so. If you withdraw your consent and we are not otherwise legally permitted to process such data, we will not continue to process this information for those purposes, but it will not impact the validity of any processing undertaken before you withdrew your consent.

We do not need your consent if we use special category data in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law.

How we will use your data

We may use your personal data to:

consider your application	<p>this will include to:</p> <ul style="list-style-type: none"> • communicate with you and any employment agency • check your identity • assess your suitability to work for us • conduct screening, assessments and interviews • make offers and provide contracts of employment or contracts to provide services • conduct pre-employment or work checks, including determining your legal right to work • carry out criminal record, credit and fraud checks • check the information you have provided • maintain a library of correspondence
manage our relationship with you	<p>this will include to:</p> <ul style="list-style-type: none"> • communicate with you • facilitate communications between you and other people • assess your continued suitability to work for us including undertaking criminal record, credit and fraud checks periodically throughout the employment or work relationship • administer the contract we have with you including: <ul style="list-style-type: none"> - making payments to you and third parties - providing and administering benefits - recording, paying and managing expenses • administer flexible working arrangements • ensure your health and safety and make reasonable adjustments for any disabilities • provide Human Resources administration, support and case management; • record, manage and report on gifts and hospitality you receive • record, manage and report on any conflicts of interest or potential conflicts of interest • train and develop you • monitor and manage your performance and adherence to our policies and procedures • resolve issues, grievances and disputes

manage our relationship with you (continued)	<ul style="list-style-type: none"> • undertake investigations, audits and internal reviews • update, consolidate and improve the accuracy of our records • correct inaccurate data held by us and third parties • control, authorise, grant, administer, monitor and terminate access to, or use of, our or third party facilities, records, infrastructure, information and communications systems • monitor telephone, email and internet use • obtain your feedback and undertake market research • maintain a library of correspondence • provide and administer employee incentive arrangements in which you participate
identify and prevent financial crime	<p>this will include to:</p> <ul style="list-style-type: none"> • detect, prevent, investigate and/or report suspected money laundering, fraud, bribery, corruption and other crime
manage and administer our information technology (IT)	<p>this will include to:</p> <ul style="list-style-type: none"> • identify, report, manage and resolve faults • administer, support, develop, manage and maintain our IT
meet our legal contractual and regulatory obligations	<p>this will include to:</p> <ul style="list-style-type: none"> • comply with HMRC, Health and Safety requirements and immigration obligations • comply with the requirements to make reasonable adjustments • provide information to our auditors and/or other third parties acting on our behalf, for the purposes of collating data required for, or preparing statutory reports • identify if you, a close associate or relative are subject to financial sanctions or are considered a politically exposed person • complying with the requirements of and requests from our regulators (including the FCA and PRA) including providing to them information: <ul style="list-style-type: none"> - about allegations of misconduct and/or capability - the remuneration of directors and persons performing senior manager and certification functions - to assist with any investigation • carry out checks required for regulatory purposes
manage, run and develop our business	<p>this will include to:</p> <ul style="list-style-type: none"> • plan the use and future use of our resources including resource, recruitment, restructuring and succession planning • develop our workforce including education, training and certification • develop, plan and administer the benefits we offer • prepare budgets and financial plans • prepare reports and undertake analysis • manage risk to us, you, our suppliers, shareholders, customers and clients • share data about you and your employment or your engagement with us with: <ul style="list-style-type: none"> - our regulators and ratings agencies; - our investors or potential investors, funders and their advisers, and - any prospective purchaser of us or part of us, seller to us or party seeking to merge with us or any person who does or wishes to fund or otherwise be involved in any such transaction and their representatives • prepare our annual report and accounts • provide data, reports and returns to our regulators, other statutory bodies, our trade bodies or when required by a court order or other legal or contractual obligation • manage, monitor, analyse, develop, forecast and report on the performance of our businesses, suppliers and other third parties including accounting and auditing • seek advice from our advisers • pay fees to, and recover fees from, employment agencies and provide them with information about your application or work with us • comply with any other legal obligation imposed on us, including where you have sought to exercise your legal rights

investigate and respond to complaints, disputes and where necessary to bring or defend legal claims	<p>this will include to:</p> <ul style="list-style-type: none"> • identify and document facts and evidence • investigate and respond to complaints, disputes, regulatory investigations and/or to bring or defend legal claims • allow us to ensure that we offer the highest standard of service, by identifying if we have provided any inadequate service and the causes of such failings, and to determine how to avoid any repeat of that situation and improving our services
---	--

Call recording

We will record and/or monitor telephone calls for the following purposes:

- for security, quality and/or training purposes;
- to confirm that you have complied with our instructions and training;
- to resolve or investigate any complaints, queries or concerns;
- to comply with our legal obligations, and
- to prevent fraud or other criminal activities.

The legal grounds on which we will process your data

We will only process your personal data if we have a reason to do so that is legally permitted. When using your personal data for the purposes listed above we are relying on one or more of the following legal reasons for processing that data:

- the purpose is necessary for the performance of a contract with you or, if you asked us to, to enable us to enter into a contract with you;
- the purpose is necessary for us to comply with our legal obligations;
- the purpose is necessary for our legitimate interests, or
- if you have consented to us processing personal data for one or more specified purposes.

The legitimate interests we have for processing your personal data as described above include to:

- comply with our legal and contractual obligations, best practice, internal policies and codes of practice;
- exercise our legal rights;
- verify the information provided to us to ensure its accuracy;
- manage and develop the benefits we provide to our workforce;
- develop and improve our business;
- ensure we have sufficient information to consider any application for employment or work;
- ensure that our employees, temporary workers and contractors meet and continue to meet the standards, values, ethics and behaviours we expect;
- manage and reduce risks to you, our business, suppliers, shareholders, customers and clients;
- prevent crime including financial crime and money laundering;
- prevent unauthorised access or use of our premises, IT, systems and resources;
- undertake analysis, modelling, and forecasting;
- keep our records up to date;
- be efficient in running our business, providing our products and services, fulfilling our legal obligations and meeting expectations of us;
- train and develop our employees and other people who work with us;
- ensure our business is profitable and has adequate levels of capital and funding, or
- facilitate investment in, and the growth of, our business.

Any special category data will only be processed where it is lawful to do so and shall potentially include processing:

- with your prior explicit consent;
- where necessary for health or social care purposes;
- where permitted by law to protect your well-being;
- where necessary for equal opportunities monitoring;
- to prevent or detect unlawful acts;
- for the protection of the public;
- for the provision of confidential counselling, advice or support services where necessary;
- for insurance purposes; or
- for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Any personal data on criminal convictions will only be processed to the extent required by law and regulation or as otherwise permitted to:

- prevent fraud;
- to comply with our legal obligations under anti Money Laundering and Financial Sanctions Legislation;
- decide whether to offer or terminate your employment or engagement with us, or
- notify the PRA and FCA in circumstances we believe there has been a breach of Conduct Rules or your role falls under the Senior Managers and Certification Regime and that amounts to a material change to fitness and propriety.

Who we share your data with

Your data may be shared internally, including with members of the HR team, your line manager, managers in the business area in which you work, directors, IT staff and other business areas if access to the data is necessary for the performance of their roles.

We will also share your data with other companies within the Charter Court Group and with:

- you, your advisers and representatives;
- employment agencies;
- your referees and previous employers when obtaining pre-employment or work references or updated employment references;
- your bank, building society, mortgage lender and landlord;
- our bank and BACS;
- credit reference agencies and fraud prevention agencies;
- Higher Education Degree Check (HEDD);
- agents and suppliers who act or may act on our behalf for example our payroll provider for the provision of payroll services;
- companies which provide benefits including pension, childcare vouchers, SAYE, Share Incentive Plan, employee incentive plans, the trustee of any employee benefit trust established by Charter Court Group, life assurance, private medical insurance and dental cover, group income protection, group critical illness, car insurance (where applicable);
- the providers of general practitioner, consultant and/or occupational health and counselling services;
- our engagement survey providers for the provision of periodic employee engagement surveys;
- our advisers including but not limited to external advisers, lawyers, accountants and auditors;
- our insurers;
- the courts and any arbitrator or adjudicator of a dispute involving us;
- companies providing training to you or accreditors of training we offer;
- statutory and regulatory bodies including the Disclosure and Barring Service, tax authorities, HMRC, the Benefits Agency, Information Commissioner's Office, PRA, FCA, Health and Safety Executive and Bank of England;
- law enforcement agencies and other agencies;
- credit rating agencies;
- market research companies;
- any investor, potential investor, funder, purchaser in or of our business or any part of our business and their advisers;
- any business with which we are seeking to merge and their advisers, or
- any other person you ask us to provide information to.

How long we will hold your data for

We will usually keep your personal data until the later of six months from the date of your enquiry about or application for a vacancy or potential vacancy and seven¹ years from the end of your employment by, or work with us. We may retain the data for longer where it is necessary for us to do so to meet our legal or regulatory obligations, for research or statistical purposes or technical reasons.

Credit reference agencies

In order to process your application for employment or work with us and to assess your continued suitability to work for us, we will perform credit and identity checks on you with a credit reference agency (CRA).

To do this, we will supply your personal data to the CRA and they will give us data about you. This will include information about your financial situation and financial history. The CRA will supply to us both public (including the Electoral Register) and shared credit, financial situation and financial history information and fraud prevention information.

We will use this information to:

- verify your identity and address;
- assess your creditworthiness;
- verify the accuracy of the data you have provided to us, and
- prevent criminal activity, fraud and money laundering.

When the CRA receive a search from us they will place a search soft footprint on your credit file that may be seen by others undertaking a credit search including lenders.

The identity of the CRA, their role also as a fraud prevention agency, the data they hold, the ways in which they use and share personal data, data retention periods and your data protection rights with the CRA are explained in more detail at <http://www.experian.co.uk/crain/index.html>

Fraud prevention agencies

When you apply for a role with us and during the course of your employment or work with us we will check your details against the Cifas databases established for the purpose of allowing organisations to record and share data on their fraud cases, other unlawful or dishonest conduct, malpractice, and other seriously improper conduct ("Relevant Conduct") carried out by their staff and potential staff. "Staff" means an individual engaged as an employee, director, trainee, homeworker, consultant, contractor, temporary or agency worker, or self-employed individual, whether full or part time or for a fixed-term.

The personal data you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and other relevant conduct and to verify your identity.

Details of the personal information that will be processed include: name, address, date of birth, any maiden or previous name, contact details, document references, National Insurance Number and nationality. Where relevant, other data including employment details will also be processed.

We and Cifas may also enable law enforcement agencies to access and use your personal data to detect, investigate, and prevent crime.

We process your personal data on the basis that we have a legitimate interest in preventing fraud and other Relevant Conduct, and to verify identity, in order to protect our business and customers and to comply with laws that apply to us. This processing of your personal data is also a requirement of your engagement with us.

Cifas will hold your personal data for up to six years if you are considered to pose a fraud or Relevant Conduct risk.

¹ 10 years for directors and persons performing the PRA/ FCA's senior manager and certification functions

Consequences of processing

Should our investigations identify fraud or any other Relevant Conduct by you when applying for, or during the course of your, employment/ engagement with us, your employment/ engagement may be refused or your existing contract of employment or engagement may be terminated or other disciplinary action taken (subject to your rights under your existing contract and under employment law generally).

A record of any fraudulent or other Relevant Conduct by you will be retained by Cifas and may result in others refusing to employ you. If you have any questions about this, please contact us using the details provided.

Data transfers

Should Cifas decide to transfer your personal data outside of the European Economic Area, they will impose contractual obligations on the recipients of that data to protect your personal data to the standard required in the European Economic Area. They may also require the recipient to subscribe to 'international frameworks' intended to enable secure data sharing.

If you choose not to give us personal data

You have to provide certain data, such as contact details and your right to work in the UK to enable us to consider your request to work for us. If you do not provide this data it will hinder our ability to consider your request and administer the rights and obligations arising as a result of our relationship efficiently.

You have obligations under your employment contract or contract to provide services to provide us with data. In particular, under your employment contract you are required to report absences from work and may be required to provide data about disciplinary or other matters under the implied duty of good faith which is a term implied by law in your contract with us. If you do not provide that data, you will be in breach of your contract with us.

You may also have to provide us with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Your legal rights

You have a number of rights over your personal data processed by us. These include your rights to request:

- **access to your personal data.** You may request a copy of the personal data that we hold about you.
- **accuracy of your personal data.** You may request that we correct incomplete, inaccurate or outdated personal data. We take sensible steps to make sure that personal data is accurate, complete, and current. You can help us do this by notifying us of any changes to your personal data.
- **transmission of personal data.** You may request that we transfer personal data you have provided to us to you or to another person.
- **erasure of personal data.** You may request that we delete your personal data.
- **that the processing of your personal data be restricted.** You may request that our use of your personal data ends, is restricted or limited.
- **the withdrawal of your consent.** In the limited circumstances where you have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, you have the right to withdraw your consent for that specific processing at any time.

The extent of these rights are limited by law and we may not act on part or all of your request(s) where the right(s) are not applicable. If we do not act on your request we will explain our reasons for not doing so when responding to your request.

If you require any further information about how we handle your personal data or if you wish to make a request to exercise any of your rights under applicable Data Protection Laws, please contact our Data Protection Officer.

Sending your personal data outside the EEA.

Your personal data may be processed or transferred outside the United Kingdom and the European Economic Area.

If you require further information as to where your personal data is transferred to, and the measures we have implemented to safeguard that information, please contact our Data Protection Officer.

How to complain

If you are unhappy with the outcome of any of your requests to exercise your rights, or how we handle your personal data then please let us know.

You are also entitled to complain with the Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Email: Casework@ico.org.uk

Tel: 0303 123 1113