

## **CHARITY BANK FAIR PROCESSING NOTICE**

*This Fair Processing Notice relates to our processing of your personal data as an applicant for a role at Charity Bank as an employee, worker or contractor. Please refer to the Privacy Notice on our website ([www.charitybank.org/privacy](http://www.charitybank.org/privacy)) to find out more about how we process your personal data when you visit our website and/or attend our events and/or connect with us via social media and/or become a Charity Bank customer. If you are successful in your application, you will also be provided with access to the Fair Processing Notice applicable to employees, workers and contractors.*

### **Purpose**

Charity Bank is committed to protecting the privacy and security of your personal information.

This Fair Processing Notice describes how we collect and use personal information about you during your recruitment application process with us, in accordance with the General Data Protection Regulation (GDPR). It applies to all employees, workers and contractors.

This notice does not form part of any offer letter, contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read and retain this notice, together with any other Fair Processing Notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information and what your rights are under data protection legislation.

### **Data Controller**

Charity Bank is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this Fair Processing Notice.

Charity Bank is registered with the Information Commissioner's Office (ICO) as a Data Controller. Our registration number is Z6540626 and you can find details of our registration [here](#). We review and update our register entry every year.

### **Data Protection Lead**

If you have any queries relating to Charity Bank's registration as a data controller and/or its use of your personal data, you should contact our Data Protection Lead at [GDPR@charitybank.org](mailto:GDPR@charitybank.org).

### **Data protection principles**

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.

3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

### **The kind of information we hold about you**

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection, such as information about a person's health or ethnicity.

All of the information you provide during the process will only be used for the purpose of progressing your application, or to fulfil legal or regulatory requirements if necessary.

We will not share any of the information you provide during the recruitment process with any third parties for marketing purposes or store any of your information outside of the European Economic Area. The information you provide will be held securely by us and/or our data processors whether the information is in electronic or physical format.

We will use the contact details you provide to us to contact you to progress your application. We will use the other information you provide to assess your suitability for the role you have applied for.

We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary.

The information we ask for is used to assess your suitability for employment. You don't have to provide what we ask for but it might affect your application if you don't.

During the application process we will ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, referees and for answers to questions relevant to the role you have applied for. Our HR team will have access to all of this information. You may also be asked to provide equal opportunities information. This is not mandatory information – if you don't provide it, it will not affect your application. This information will not be made available to any staff outside of our HR team, including hiring managers, in a way which can identify you. Any information you do provide, will be used only to produce and monitor equal opportunities statistics.

Our hiring managers then shortlist applications for interview. At this stage they will be provided with a copy of your application, but not any equal opportunities information.

At the interview stage, you may be invited to complete tests or occupational personality profile questionnaires and/or to attend an interview – or a combination of these. Information will be generated by you and by us. For example, you might complete a written test and we will take interview notes. This information is held by us, accessible by the HR team and the hiring manager and others present at the interview.

Final recruitment decisions are made by hiring managers and members of the HR team. All of the information gathered during the application process will be taken into account. You are able to ask about decisions made about your application by speaking to your contact in our HR team or by emailing [recruitment@charitybank.org](mailto:recruitment@charitybank.org).

### Offer of employment

If we make an offer of employment, this will be dependent upon you successfully completing pre-employment checks which include, but are not limited to, satisfactory references, proof of identity, proof of eligibility to work in the UK.

You will therefore be required to provide:

- **Proof of your identity** – you will be asked to attend our office with original documents, we will take copies.
- **Proof of your qualifications** – you will be asked to attend our office with original documents, we will take copies.
- **Bank details** – to process salary payments.
- **Emergency contact details** – so we know who to contact in case you have an emergency at work.
- **Declarations of interests** - we will ask you to confirm details of any organisations within which you are a director or trustee and/or a shareholder to the extent that this may have an impact on your potential role.
- We will contact you to **complete an application** for (i) a **Criminal Record check** via the Disclosure and Barring Service, which will verify your declaration of unspent convictions and (ii) an **Adverse Credit Check**, which will check that there is no evidence of financial mismanagement, by searching records of County Court Judgements, bankruptcies, voluntary arrangements, decrees, administration orders and similar.
- We will **contact your referees**, using the details you provide in your application, directly to obtain references. This may include a formal application for a regulatory reference.

To summarise, during the whole process from receipt of your application to issue of an offer to work with/for us, we will collect, store, and use the following categories of personal information about you:

- **personal contact details** - such as your address, telephone number(s), personal email addresses, details of any company through which you provide services and your connection to that company;
- **identifying or authenticating data** - such as your name, data of birth, employee number, payroll number, National Insurance number, copy driving licence, copy passport, copies of right to work documentation, copy utility bills and photographs; and
- **professional data** - such as job titles, education, qualifications/accreditation, work history, references, information included in a CV or cover letter, training records and professional memberships.

We may also collect, store and use the following "**special categories**" of more sensitive personal information:

- information you have provided to us about your **race or ethnicity**;
- information about your **health**, including any medical condition, but only where relevant to your job application and potential recruitment; and
- information about **criminal convictions and offences** to the extent that this information is provided to us as a result of any Disclosure and Barring Service check required by our regulator.

## **How is your personal information collected?**

We collect personal information about job applicants through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies, such as the Disclosure and Barring Service.

If you become an employee, worker or contractor, we will collect additional personal information in the course of job-related activities throughout the period of you working for us, but this is outside the scope of this Fair Processing Notice and, if successful, you will be provided with access to the Fair Processing Notice for employees, workers and contractors.

## **How we will use information about you**

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

1. Where we need to perform the contract we have entered into with you.
2. Where we need to comply with a legal obligation.
3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

We may also use your personal information in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else's interests).
2. Where it is needed in the public interest or for official purposes.

## **Situations in which we will use your personal information**

The table overleaf details the types of personal data we would typically collect, our grounds for processing that data and your associated rights.

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. If you are successful, we will usually hold the data you have provided during the application process as part of your employee file. We would usually hold this data for a maximum of 6 years following the end of the employment relationship, unless exceptional circumstances require otherwise. If you are unsuccessful at any stage of the process, the information you have provided until that point will be retained for 6 months from the closure of the recruitment campaign (unless you have agreed that we can keep your details on file for longer).

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with applicable laws and regulations.

<b>Your situation</b>	<b>Personal data we would typically hold</b>	<b>Our grounds for processing your data</b>	<b>Your rights</b>
<b>Prospective employee, worker, freelance contractor (individual) or volunteer</b>	Name, address, email address, phone number, date of birth (if provided), CV (may include professional membership, education, qualifications/accreditation, evidence of DBS check (if relevant and if portable)), references from previous employers (including regulatory references where relevant), other sensitive personal data to the extent that you choose to share this with us. <sup>1</sup>	Legitimate Interests	Access Correction/Rectification Deletion Object to/Restrict processing (No right to portability)

### **Change of purpose**

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

### **How we use particularly sensitive personal information**

"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy document and safeguards which we are required by law to maintain when processing such data. We may process special categories of personal information in the following circumstances:

1. In limited circumstances, with your explicit written consent.
2. Where we need to carry out our legal obligations or exercise rights in connection with employment.
3. Where it is needed in the public interest, such as for equal opportunities monitoring.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities, with the appropriate safeguards.

<sup>1</sup> **NB** - This list includes both "criminal conviction" data and "special category" data. These sets of data are being processed on all the grounds specified in the next column and meet, as relevant, the following required conditions: (i) consent (in particular, DBS checks, and the sharing of medical information with line-managers/HR team), (ii) to be used in bringing or defending legal claims, (iii) to assess the working capacity of the employee and (iv) to carry out the obligations and to exercise the specific rights of the controller or data subject in the field of employment law.

## **Our obligations as a potential employer**

We will use your particularly sensitive personal information in the following ways:

- if successful, we will use only information which you have provided about your physical or mental health, or disability status, to provide appropriate workplace adjustments before you start with us; and
- if you have provided us with information about your race or national or ethnic origin, religious, philosophical or moral beliefs we will only use this to ensure meaningful equal opportunity monitoring and reporting.

## **Do we need your consent?**

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

## **Information about criminal convictions**

We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our regulatory and legal obligations.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We envisage that we will hold information about criminal convictions because our regulator requires us to carry out Disclosure and Barring Service checks as part of the recruitment process and at regular intervals during the course of you working for us. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so.

## **Automated decision-making**

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making. We will notify you in writing if this position changes.

## **Data sharing**

We may have to share your data with third parties, including third-party service providers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal information outside the EU.

If we do, you can expect a similar degree of protection in respect of your personal information.

## Why might you share my personal information with third parties?

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

From time to time we may involve a third party in the collection or processing of personal data. Where we regularly involve a third party in the processing of personal data, we will include their details in this document.

We only work with third parties which meet our stringent procurement criteria. Under these criteria we review not only their ability to provide the goods or services we require but also their general ethos (commitment to the charity/social sector) and working practices. Before we work with a third party on a new project involving the processing of personal data, we will carry out a Data Protection Impact Assessment. We will also ensure that the terms of the contract with any third-party data processor meet the legal requirements imposed by the GDPR.

The table below identifies all third-party service providers involved in the handling of your personal information as an applicant, pending confirmation of appointment as an employee, worker or contractor of Charity Bank as at the date of this Notice. Depending upon the level of service these organisations provide to us, they may be acting as data processors for us:

Name	Purpose / Comment
CascadeGo	HR system ( <i>annual leave and sickness records, policies and procedures, staff directory</i> )
NatWest	Credit Card provider
UCheck	Adverse Credit Checks and Disclosure & Barring Service checks

We are in discussions with all our service providers who act as data processors for us to obtain a commitment from them that they will:

- only process Personal Data in accordance with our written instructions;
- put in place appropriate technical and organisational measures (which we will have the right to check) to protect against unauthorised or unlawful processing of that Personal Data and to protect against accidental loss or destruction of or damage to Personal Data;
- ensure that all personnel who have access to and/or process Personal Data are obliged to keep that Personal Data confidential;
- not transfer any Personal Data outside the EEA unless we have already agreed to this in writing; and the service provider agrees to (i) provide appropriate safeguards; (ii) provide an adequate level of protection to any Personal Data which is transferred; (iii) ensure the Data Subject's rights are not adversely affected; and (iv) meet any additional conditions required by us;
- assist us in promptly dealing with and responding to any Data Subject request;
- notify us within 48 hours of any suspected or actual Personal Data breach;
- at our request, delete and/or return Personal Data on termination of the contract other than to the extent we have agreed the service provider may retain that Personal Data for audit purposes;
- maintain records demonstrating compliance with these obligations;
- indemnify us against any loss arising out of or in connection with the service provider's processing of Personal Data on our behalf and its obligations as a Data Processor; and
- maintain in force a sufficient level of insurance to cover its liabilities to us.

## How secure is my information with third-party service providers and other entities in our group?

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

### What about other third parties?

On occasion, we will be required to share your personal data with third parties for regulatory and audit purposes. We will only share the minimum amount of detail required for the purpose and will anonymise records where we can. These third parties are subject to duties of confidentiality and they will not be permitted to share your data outside their own organisation other than in exceptional circumstances, such as where there is an overriding public interest, including the prevention or detection of crime. Details of our current auditors are listed in our Annual Accounts - currently [Deloitte](#) and [KPMG](#) - and our regulators are the [Prudential Regulation Authority](#), the [Financial Conduct Authority](#) and the [Information Commissioner's Office](#). We also send information to the [Department for Business, Energy & Industrial Strategy](#), to enable us to maintain our licence to offer Community Investment Tax Relief to eligible depositors/investors. You may click on the hyperlinks given in this paragraph to be directed straight to their Fair Processing Notices.

### Data security

We have put in place measures to protect the security of your information. For more details please contact our IT Manager.

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

We take all reasonable steps to protect your personal data through technological means and internal processes. All personal data we receive is stored either electronically or in paper format in our internal systems which are secure and cannot be accessed by external parties without our authorisation. We do not give out personal information on the telephone or by email unless you have requested that we do so and we have verified that it is you making the request. We regularly back-up the data which we hold and ensure that these back-ups are subject to an equivalent level of technological and organisational safeguards as the original data. We regularly test the resilience of our systems and make adjustments as required.

As you would expect, some of our IT suppliers are large international companies, but as they are processing the Personal Data of EU citizens, they are required to adhere to the requirements of the GDPR. You may request further information about our IT systems and approach to information security (including a list of our third-party suppliers) by contacting [gdpr@charitybank.org](mailto:gdpr@charitybank.org).



We will only give authorisation to third parties to access our systems where they are providing a service to us under a written contract which includes terms requiring them to protect your data. These services may include: internal/external audit, IT consultancy (software/hardware) or IT advisory services (user support). We ask all our IT suppliers to go through a rigorous procurement exercise to ensure they meet our requirements in terms of protecting your data. As you would expect, our ability to negotiate contractual terms with larger companies may be extremely limited. In this situation we will take all reasonable steps to protect your data.

We limit the processing of data outside the European Economic Area (EEA). For a current list of countries in the EEA, please see the list [here](#). All our own IT systems and back-up systems rely on data-centres located within the European Union (EU) (a smaller set of countries than the EEA). Where we use the services of a third party which requires the transmission or handling of personal data outside the EU we will notify you, by including the relevant details within this Fair Processing Notice. Whilst the GDPR has effect on all organisations (wherever they are located) which process the personal data of EU citizens, we do take steps to ensure, through due diligence and contractual terms, that the third-party supplier is committed to a high standard of data protection compliance.

### **Your duty to inform us of changes**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

### **If you fail to provide personal information**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

### **Your rights in connection with personal information**

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it.
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.
- **Request the transfer** of your personal information to another party.
- **Right to withdraw consent** - in the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific

purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact our Data Protection Lead at [gdpr@charitybank.org](mailto:gdpr@charitybank.org). Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our HR Manager in writing.

You will not have to pay a fee to access your personal information (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is extensive. Alternatively, we may refuse to comply with the request if your request is clearly unfounded or excessive.

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

### **Changes to this Fair Processing Notice**

We reserve the right to update this Fair Processing Notice at any time, and we will provide you with a new Fair Processing Notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

### **Making a complaint**

Charity Bank tries to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate. We would also welcome any suggestions for improving our procedures.

If you want to make a complaint about the way we have processed your personal information, you can contact the Data Protection Lead at the address given above. Please provide as much detail as possible to help us to review your concerns.

When you submit a data protection complaint we will deal with this as quickly as we can and, in any event, within relevant statutory timeframes. Please remember that we will be able to respond more quickly if you provide evidence of identity with your query as we cannot provide our response until we are sure we are releasing it to the right person.

When we receive a complaint from a person, we make up a file containing the details of the complaint. This normally contains the identity of the complainant and any other individuals involved in the complaint.

We will only use the personal information we collect to process the complaint and to check on the level of service we provide. We do compile and share statistics showing information like the number of complaints we receive with our regulators, but not in a form which identifies anyone.

We usually have to disclose the complainant's identity to whoever the complaint is about. This is inevitable where, for example, the accuracy of a person's record is in dispute. If a complainant

doesn't want information identifying him or her to be disclosed, we will try to respect that. But it may not be possible to handle a complaint on an anonymous basis.

We will keep personal information contained in complaint files in line with our retention policy. This means that information relating to a complaint will be retained for a maximum of six years from closure. It will be retained in a secure environment and access to it will be restricted according to the 'need to know' principle.

Similarly, where enquiries are submitted to us, we will only use the information supplied to us to deal with the enquiry and any subsequent issues and to check on the level of service we provide.

### **Right to complain to the Information Commissioner's Office**

If have a concern about the way in which we are Processing your Personal Data and we have not been able to resolve that concern directly with you, you may complain to the Information Commissioner's Office (ICO). You may call the helpline on 0303 123 1113. Further details about how to submit a report to the ICO can be found [here](#).

**If you have any questions about this Fair Processing Notice, please contact our HR Manager.**