Hampshire Trust Bank

Fair Processing Notice for Employees and Applicants

About this Fair Processing Notice

In this Fair Processing Notice we explain:

Note: You have the right to object to us processing your personal data - please see section 9(e) below

1. Who we are

We are Hampshire Trust Bank Plc. We are a bank registered in England and Wales under company number 01311315 and we have our registered office at 55 Bishopsgate, London EC2N 3AS. We are authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority. Our FRN is 204601.

We are the **data controller** for information that you provide to us and of information that we hold about you from third parties.

2. Our Data Protection Officer and how to contact our Data Protection Officer

Our Data Protection Officer is Scott Southgate.

You can contact our Data Protection officer in one of the following ways:

- by writing to our Data Protection Officer at Data Protection Officer, Hampshire Trust Bank plc, 55 Bishopsgate, London EC2N 3AS
- by sending an e-mail to our Data Protection Officer at dataprotectionofficer@htb.co.uk

3. What kinds of personal data we collect and hold about you and where we get it from

Where you are an applicant for employment, our employee or a person who applies or is employed through a personal service company we will collect and process the following types of personal data about you:

- Information about you, for example, name, address, date of birth, marital status, nationality, gender, preferred language, details of any disabilities, work restrictions and/or required accommodations.
- Information to contact you at work or home, for example, name, address, telephone, and e-mail addresses.
- Information about who to contact in a case of emergency (yours or ours), for example, name, address, telephone, e-mail addresses and their relationship to you.

- Information to identify you, for example, photographs, passport and/or driving license details and electronic signatures.
- Information about your suitability to work for us, for example, references, interview notes, work visas, ID information such as passport details and driving licence information, records/results of pre-employment checks, including criminal record checks, credit and fraud checks.
- Information about your skills and experience, for example, CVs, resumes and/or application forms, references, records of qualifications, skills, training and other compliance requirements.
- Information about your terms of employment with us, for example, letters of offer and acceptance of employment and your employment contract.
- Information that we need to pay you, for example, bank account details, national insurance or social security numbers (where applicable).
- Information that we need to provide you with benefits and other entitlements, for example, length of service information, health information and leave requests.
- Information to allow you to access our buildings and systems, for example, Employee identification number, computer or facilities access and authentication information, identification codes, passwords, answers to security questions, photographs and video images.
- Information relating to your performance at work, for example, performance ratings, leadership ratings, targets, objectives, records of performance reviews, records and/or notes of 1 to 1s and other meetings, personal development plans, personal improvement plans, correspondence and reports.
- Information relating to discipline, grievance and other employment related processes, for example, Interview/meeting notes or recordings, correspondence.
- Information relating to your work travel and expenses, for example, bank account details, passport, driving licence, vehicle registration and insurance details.
- We obtain information about you from a number of sources, such as:
    - recruitment agents who send us your information,
    - your previous employers such as in connection with references,
    - the regulator, if we are required to obtain information from them such as in connection with regulatory references,
    - financial crime agencies,
    - health information, for example where you complete a work related health questionnaire to assist us to determine any employee support requirement,
    - employee screening and reference checking agencies to check that the information that you have given to us is accurate,
    - our office facilities management for example in connection with building access and security,
    - potentially, solicitors and other external advisors where, for example, this relates to disputes,
    - salary payment providers, for example information about payments and tax status.

4. Why we collect your personal data and what we use it for

We collect and process your personal data:

- For recruitment purposes, for example:
    - to assess your suitability to work for us;
    - to perform requisition and applicant management activities;
    - to perform precision matching to job vacancies;
    - to conduct screening, assessments and interviews;
    - to maintain a library of correspondence;
    - to make offers and provide contracts of employment;
    - to conduct pre-employment checks, including determining your legal right to work and carrying out criminal record and credit checks where applicable.
- For HR, finance and other business administration purposes, for example:
    - staffing, including resource planning, recruitment, termination, and succession planning,
    - budgetary and financial planning and administration;
    - organisational planning and development and workforce management;

  - compensation, payroll, and benefit planning and administration, including salary, tax withholding, tax equalisation, awards, insurance and pensions;
  - workforce development, education, training and certification;
  - performance management;
  - problem resolution, including carrying out internal reviews, grievances, investigations, audits;
  - business travel and expense management;
  - to conduct business reporting and analytics;
  - administration of flexible work arrangements;
  - administration of employee enrolment and participation in activities and programmes offered to eligible employees, including matching donations to non-profit organisations, and wellness activities;
  - work-related injury and illness, including the management of employee Health & Safety, and disabilities;
  - to provide HR helpdesk support and case management;
  - to communicate with you and to facilitate communication between you and other people;
  - compliance and compliance reporting, including conflict of interest and gifts and hospitality reporting;
  - risk management;
  - project management;
  - training and quality purposes.
- For security purposes, for example:
  - physical access control;
  - authorising, granting, administering, monitoring and terminating access to or use of our facilities, records, property and infrastructure including communications services such as business telephones and email/internet use;
  - CCTV; and
  - prevention and detection of crime;
- for IT administration purposes, for example, IT systems access control and use monitoring;
  - IT fault reporting, management and resolution;
  - systems administration, support, development, management and maintenance.
- to meet our legal obligations.
- to protect and defend our legal rights

5. The legal basis upon which we collect, process and store your personal data

The UK's data protection law allows the use of personal data where its purpose is legitimate and isn't outweighed by the interests, fundamental rights or freedoms of data subjects. The law calls this the **legitimate interests** condition for personal data processing.

As explained above, we only collect, use and store the minimum amount of personal data about you that is necessary for us to consider employing you, in order to manage our employer/employee relationship and to comply with our legal and regulatory obligations arising as a result of us employing you. Accordingly, the basis upon which we collect, use and store your information is because we have a **legitimate interest** to do so as a regulated bank employing you.

Our legitimate interests include:

- to act as a prudent and responsible lender and financial institution,
- to undertake reference checks, credit checks and risk assessments,
- to help combat financial crime including tax evasion, bribery, fraud and money-laundering,
- to maintain network and information security,
- to recruit and maintain the best employees,
- to meet our legal and regulatory obligations,
- to protect and defend our legal rights,
- to maintain accurate records,
- to pursue our commercial objectives as a bank where this does not override your rights and freedoms as a data subject.

When we process your personal information for our legitimate interests, we make sure to consider and balance any potential impact on you (both positive and negative), and your rights under data protection laws. Our legitimate business interests do not automatically override your interests - we will not use your Personal Data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law).

6. Where your personal data is stored and processed

We are based in the UK, and we keep our filing systems and databases here.

We may be required to send or allow access to personal data from elsewhere in the world. This might be the case, for example, when someone providing support services to us is based overseas or uses overseas data centres.

While countries in the European Economic Area all ensure a high standard of data protection law, some parts of the world may not provide the same level of legal protection when it comes to personal data. As a result, if we do send personal data overseas we will make sure suitable safeguards are in place in accordance with European data protection requirements, to protect the data. For example, these safeguards might include:

- Sending the data to a country that's been approved by the European authorities as having a suitably high standard of data protection law. Examples include the Isle of Man, Switzerland and Canada.
- Putting in place a contract with the recipient containing terms approved by the European authorities as providing a suitable level of protection.
- Sending the data to an organisation which is a member of a scheme that's been approved by the European authorities as providing a suitable level of protection. One example is the Privacy Shield scheme agreed between the European and US authorities. Another example is Binding Corporate Rules.

If your data has been sent overseas like this, you can find out more about the safeguards used from us.

Whenever fraud prevention agencies transfer your personal data outside of the European Economic Area, they 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.

7. Who we share your personal data with, what personal data we share and why we do so

We do not sell any of your information to third parties, we will not give anyone your information so that they can market to you.

- **Printers**

  We may use professional printers to print the account statements, letters and other documents that we send to you from time to time and so we have to share with them the information that needs to be printed into those statements, letters and documents that you receive.

- **Credit Reference Agencies and Fraud Prevention Agencies**

  In order to receive credit and financial crime check information about you from credit reference agencies we are required, on a reciprocal basis, to share information about you with those credit reference and fraud prevention agencies.

  We will pass your details on to credit reference agencies and fraud prevention agencies and we will receive scores and reports from them. You will receive a copy of the Credit Reference Agency Information Notice when you make an application to us which will explain how the three main credit reference agencies Callcredit, Equifax and Experian each use and share personal data they receive about you and/or your business that is part of or derived from or used in credit activity. You can also download or read it by visiting http://www.experian.co.uk/crain/

We and fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime. Please note that fraud prevention agencies can hold your personal data for different periods of time, and if you are considered to pose a fraud or money laundering risk, your data can be held for up to six years.

If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to employ you. A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to employ you. If you have any questions about this, please contact us on the details provided.

One of the fraud prevention agencies that we use is Experian. Please note the following:

a. Experian may check the details you provide to us against any particulars on any database (public or otherwise) to which Experian has access in order to carry out relevant verification services,
b. a specific (non-credit) footprint is left by Experian, and
c. a record of the Experian decision is available for us to retrieve for auditory purposes.

To find out more about Experian's operations in the identity and fraud space, please visit http://www.experian.co.uk/crain/idf-information-notice.html to read Experian's ID&F Information Notice.

- **Survey Companies**

We are constantly trying to improve our employee experience and we may use the services of an online satisfaction survey company to gather your feedback and reviews about us. To enable them to send you the e-mail survey request, we provide them with your name and e-mail address and details.

- **Regulators**

We will share information about you with our regulators in order to meet our regulatory reporting obligations. We will only share the information about you with our regulators that is necessary to meet our legal and regulatory obligations.

- **Our Auditors**

We may be required to share information about you with our auditors in order to verify to them that you are our employee, that the information in our accounts and the information that we share with our regulators is accurate.

- **Payroll Providers**

We employ third party payroll providers to pay salaries on our behalf and we will share with them information about you that is necessary to effectively process and pay your salary.

- **Employee Benefits Providers**

We may share personal data about you with third parties who provide employee benefits, such as pension providers, medical aid providers and the like.

Please rest assured that we have quality checked all the third parties to whom we send your information and have appropriate contractual arrangements in place with them to make sure that they will only use the information for the purposes that we have sent it to them and that it will be properly protected.

8. How long we will store your personal data

We will only use your information for as long as we need it in order to manage our employment relationship.

As soon as you have left our employment and we have finalised our administrative work in relation to you leaving then we will hold your information in secure storage until we are permitted by law and regulation to permanently erase it.

To comply with our current legal, regulatory and financial crime records retention obligations, we will hold your information for a period of:

(1) six years after you leave our employment;
(2) six months if you applied for employment but withdrew your application or were unsuccessful in your application;

These periods will be extended if your information is needed in relation to any civil or criminal proceedings or if we are required to hold it for longer by our regulators, law enforcement agencies or the courts.

Please note that some information is required to be held for much longer periods of times. You can find full details in our Record Retention Policy.

9. Your rights to your personal data

We recognise that your information is your information - it does not belong to us. You have a number of important rights which put you in control of your information. To help you understand your rights, we will explain them below.

a. Your right of access to your personal data

You can ask us at any time to tell you what personal data we hold about you and we will do so, without undue delay, and in any event within one month of receipt of your request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. We will tell you of any such extension within one month of receipt of your request, together with the reasons for the delay. Where you make the request by electronic means, we will provide the information by electronic means where possible, unless otherwise requested by you.

After 25 May 2018 we will not charge you any fee for providing this information (unless the request is manifestly unfounded or excessive, in which case we may charge you a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested. Alternatively, we may be entitled to refuse the request). If you request more than one copy of the information then we may charge you a reasonable fee for the administration of producing the additional copies.

We may ask you to provide us with information to verify your identity before providing you with the information requested.

b. Your right of rectification to your personal data

You have the right to have any personal data that we hold about you corrected if it is wrong or completed if it is incomplete. To have it corrected or completed, simply tell us what information is wrong or incomplete and give us the correct and complete information. We will update or complete it without undue delay. We may ask you to provide supporting evidence to verify the information you are giving to us for example, proof of address where you tell us that the address details we hold about you are wrong.

c. Your right of erasure of your personal data (also known as the right to be forgotten)

In some circumstances you have the right to have the personal data that we hold about you permanently erased. You will have this right (1) when it is no longer necessary for us to process your personal data or (2) if there is no legal basis for us to process your personal data or (3) if we unlawfully process your personal data or (4) to comply with a legal obligation to which we are subject. If you believe that any of these circumstances apply to you then please tell us and we will ensure that your personal data is permanently erased without undue delay if one of these circumstances do exist.

Where we permanently erase your personal data we will also take reasonable steps to inform any third parties to whom we have provided your personal data of your request to have the personal data erased.

d. Your right to have processing of your personal data restricted

In some circumstances you have the right to have the processing of your personal data restricted. You will have this right:

- if you tell us that your personal data is inaccurate, for a period enabling us to verify its accuracy; or
- if we are not processing your personal data lawfully and you tell us that you would rather have us restrict the processing than erase it; or
- we no longer need your personal data but you need us to store it because you need it for the establishment, exercise or defence of legal claims; or
- if you have objected to us processing your personal data, for a period enabling us to verify whether the legitimate grounds on which we are processing it override your grounds for objection.

This is not an absolute right, and your personal data may still be processed where certain grounds exist. This is:

- with your consent;
- for the establishment, exercise, or defence of legal claims;
- for the protection of the rights of another natural or legal person;
- for reasons of important public interest.

Only one of these grounds needs to be demonstrated to continue data processing.

We will consider and respond to requests we receive, including assessing the applicability of these exemptions.

We will tell you once a restriction on processing has been applied and before lifting any restriction.

Where we restrict the processing of your personal data we will also take reasonable steps to inform any third parties to whom we have provided your personal data of your request to have the personal data restricted.

e. Your right to object to the processing of your personal data

As explained in this Fair Processing Notice, we process your personal data because we have a **legitimate interest** in doing so. However, you have the right to object to us processing your personal data, on grounds relating to your particular situation. If you object then we will stop processing your personal data unless we can show compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims. For example, where we detect fraud it is unlikely that your objection may prevent us supplying that information to fraud prevention agencies and legal authorities. Another example is that it is unlikely that your objection may prevent us reporting to the regulator in relation to your employment even if you object to us processing your personal data.

The only exception to this relates to where you have previously given consent to us to market to you and you change your mind and object to us using your personal data to market to you. In this case we will without undue delay stop marketing to you and we will take your objection as a withdrawal of that consent and we will update your marketing preferences.

f. Your right to data portability

New data protection legislation also contains a right to data portability that may give consumers a right in some data processing contexts, to receive their personal data in a portable format when it's processed on certain grounds, such as consent. This is not a right that will apply to your personal data because we process your personal data on the grounds of legitimate interests.

g. Your right not to be subject to automated decision making and profiling

New data protection legislation also contains a right not to be subject to a decision based solely on automated processing. We do not make any decisions based solely on automated processing.

h. Your right to complain to the Information Commissioner

If you are not satisfied with the way that we have processed your personal data or the way that we have dealt with you when exercising any of your rights then you may follow our complaints procedure by following this link www.htb.co.uk/complaints

You may also refer your concerns to the Information Commissioner's Office (or ICO), the body that regulates the handling of personal data in the UK. You can contact them by:

1. Phone on **0303 123 1113**
2. Writing to them at **Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF**
3. Going to their website at www.ico.org.uk

10. Important information for children

We do not offer employment to children – i.e. anyone under the age of 18. However we may collect and process information about children when it is necessary and incidental to employee relationship. Examples of this include where we hold the identity information of the children of our employees or child beneficiaries for the purposes of employee benefits and insurance arrangements.

If you are a child whose personal data we hold then please be aware that this Fair Processing Notice also relates to you and you should read it so that you understand how we process your personal data.

Please note that children have the same rights to their personal data, as explained in this Fair Processing Notice, as an adult.