Contractor & Temporary Worker Privacy Notice

We regularly update this document. Make sure you have the latest version by downloading it from the intranet.

Last update: January 2022

Contractor & Temporary Worker Privacy Notice

As a contingent worker, NatWest Group (the "bank", "we", "us" and "our") collects and holds personal data which may directly or indirectly identify you (together "personal information"). We process this personal information for a range of purposes relating to Human Resources ("HR"), business activities, as well as safety and security. Natwest Holdings Ltd is the data controller of your personal information in relation to the processing activities described in this Privacy Notice. Our Data Protection Officer can be contacted by emailing HREmployeePrivacy@rbs.co.uk.

This Contractor & Temporary Worker Privacy Notice ("Privacy Notice") sets out why we collect your personal information, what information is collected and how it is processed. Throughout this Privacy Notice we use the term "processing" to cover all activities involving your personal information, including collecting, handling, storing, sharing, accessing, using, transferring, securing and disposing of information.

Why do we collect your personal information?

In order to manage your relationship with the bank, we need to process certain personal information about you for the purposes set out below:

Worker Management: day-to-day management of your relationship with us (like to order equipment for you); communication and training; auditing, assurance and risk management activities; and other general administrative operations in connection with your assignment.

Workforce Organisation & Strategy: where necessary to analyse and produce reports on our workforce and ensure compliance with the bank's policies.

Accounting for and Protecting Workers & Assets: to protect our property and assets (like our computer hardware and our systems). To safeguard our people and ensure compliance with laws, policies and contracts, we monitor activities in our premises, and on computers, devices, networks, communications and other assets and resources. See Page 5 for more information on monitoring.

Health, Safety & Security: to protect and monitor the health, safety and security of you, your colleagues and visitors to our premises.

Crime Prevention and Detection: for preventing and detecting crime, money laundering, fraud, terrorist financing, bribery and corruption, and international sanctions.

Regulatory and reporting obligations: in order to comply with applicable laws (e.g. occupational health and safety, employment laws, tax laws), including judicial or administrative orders and for regulatory submissions.

What personal information might we process?

Here are some examples of the type of personal information we may process about you. Generally, we collect personal information directly from you in circumstances where you provide personal information to us. However, in some instances, the personal information we collect has been inferred about you based on other information you have provided to us, through your interactions with us, or from third parties such as the agency with whom you are contracted. There's a full list in the schedule at the end of this notice.

Your Personal Information

- Personal details such as name, address and date of birth, personal email addresses and phone numbers;
- Education and work history including qualifications, skills;
- Emergency contacts;
- Work related information such as employee ID, RACF ID, job title, managers, and accident records;
- Photographs and images from CCTV; and
- Access details for premises (including NIACs data) and IT and details of any bank owned property you hold.

Who do we share your personal information with?

The bank may need to share your personal information with colleagues in the bank (both in the country where you work and in other countries in which we have operations) and with some external parties or associates of the bank. Some of these third parties and associates will be located outside the UK and/or the European Economic Area ("EEA").

Where we transfer your personal information outside the UK and/or EEA, we will ensure that it is protected in a manner that is consistent with how your personal information will be protected by us in the UK. This can be done in a number of ways, for instance the country that we send the information to might be approved by the European Commission; or the recipient may have signed up to a contract based on "Standard Contractual Clauses" approved by the European Commission, obliging them to protect your personal information. In other circumstances the law may permit us to otherwise transfer your personal information outside the UK and/or EEA. In all cases, however, we will ensure that any transfer of your personal information is compliant with applicable data protection

law. Information will only be shared if it is necessary or required (for example for the management of payroll information).

Internally your personal information may be shared with the following people. Access to personal information is limited to the information required by each individual to perform their role.

- All bank employees (for example work contact and basic role information such as that within internal address books);
- Those employees with managerial responsibility for you;
- Employees in HR who have responsibility for certain HR processes (for reporting and assignment management);
- Employees with responsibility for investigating issues of non-compliance with laws and regulations, internal policies and contractual requirements;
- Employees in IT and system owners who manage user access;
- Audit and Investigations in relation to specific audits/investigations; and
- Security managers for facilities / premises.

The bank may also need to share your information with certain external third parties including:

- Courts, regulators, government bodies and similar organisations as required by law (such as the FCA, PRA, HMRC or Health & Safety Executive or local equivalents);
- Corporate auditors and legal or other advisors; and
- Third-party suppliers (or potential suppliers), who provide services on our behalf;

How do we protect and retain your information?

Our HR systems are protected in accordance with the Group Security Policy Standard. Where we share information with other parties located outside your country, as a minimum, the bank will require that such personal information is protected as required by the laws of the country where you work. The bank also requires its third-party suppliers or recipients of personal information to guarantee the same level of protection as provided by the bank.

Your personal information will be retained in accordance with the bank's Managing Records Policy and our Records Retention Schedule (retention periods vary, and we may hold some information after your working relationship with the bank has ended). The retention period will be determined by various criteria including the type of record in which your information is included, the purpose for which we are using it and our legal obligations (laws or regulation may set a minimum period for which we have to keep information). We may on exception retain your information for longer periods than those envisaged in our Retention Schedules, particularly where we need to withhold destruction

or disposal based on an order from the courts or an investigation by law enforcement agencies or our regulators. This is intended to make sure that the bank will be able to produce records as evidence, if they're needed.

Monitoring

General

In order to protect you and our customers and to ensure compliance with our policies, legal and regulatory requirements, we will monitor you and your use of our IT systems (including those you access remotely) as well as your presence on the bank's premises. Further details in relation to acceptable use of IT systems are set out in the Security Policy. We work with the relevant authorities and law enforcement agencies in the investigation of serious matters. This, on occasion, may involve covert surveillance which is carried out in a lawful manner.

Why do we monitor you?

We will only undertake monitoring for the following reasons and will comply with all local laws, regulations and internal policies when doing so:

- Prevention and detection of possible criminal activity;
- Ensuring compliance with the bank's internal policies, including investigating or detecting inappropriate use of IT systems or access to premises;
- Ensuring compliance with local laws and regulations (such as insider dealing, market abuse, rate setting misconduct and anti-competitive discussions);
- Checking for viruses or other threats to our IT systems;
- Ensuring business continuity; and
- Training feedback.

What kind of activity and information will be monitored?

- Emails and instant messages sent, received and archived on bank provided devices or through the bank's email facilities;
- Internet access via the bank's networks or devices including websites visited, archived content, and social networks. This may include the duration of site visits; search terms used in any search engine and attempts to access blocked sites;
- All information stored or processed on your bank computer which may include (but is not limited to) your PC, laptop, any other computing device (including files, call history etc);
- Access to and use of IT systems, databases, document management systems;
- Any bank business activity carried out on your own device;

- Telephone calls using a bank supplied landline or mobile device (you will be advised locally if your calls are monitored);
- Your image captured by CCTV in/on the bank's premises; and
- The times and locations your security pass is used in/on the bank's premises.

What action can be taken as a result of the monitoring?

Communications (for example, emails) which are identified as potentially breaching laws, regulations or bank policies may be blocked and held from going out of the bank until they have been investigated.

What about your personal communications?

Every effort is made to ensure that personal communications which do not contain bank information are not captured by the monitoring systems. However, sometimes this could happen inadvertently. Where personal communications are captured, we will normally disregard these. However, if it appears that the communications are inappropriate and do not comply with the bank's policies and procedures, for example if they breach the bank's diversity and inclusion policies, action may be taken against you in accordance with those policies.

The bank information classification scheme does not apply to personal communications. Therefore, it is advisable to flag personal emails as 'personal' rather than 'confidential', 'secret' and so on.

Fraud prevention checks

To prevent or detect fraud, or assist in verifying your identity, we may from time to time search the bank's records and any records at fraud prevention and credit reference agencies. Should our investigations identify fraud or the commission of any other criminal offence by you (or on your part) when applying for, or during the course of your assignment with us, we will record details of this on internal and external fraud prevention databases. This information may be accessed from the country in which you work and other countries and used by law enforcement agencies and by us and other employers (and potential employers) to prevent fraud.

Regulatory screening

In order to comply with our legal and regulatory obligations in relation to anti-money laundering and sanctions restrictions, we will screen your personal information against internal databases and global sanctions lists. The screening will involve searching internal and third-party databases to ensure you are not on a global sanctions list.

To comply with our legal and regulatory obligations relating to anti-bribery and corruption, we may also perform searches and ask questions to assess whether there is a potential bribery or corruption risk to the bank based on the role being carried out and based on your personal and political associations. If there is a risk, we will look to assess what additional internal controls we need to put in place to reduce or mitigate that risk.

Your Rights

Access, Correction and Deletion

You are entitled to see the information the bank holds about you. There is information available on the Intranet about accessing your personal information, please search for “subject access requests” or send the request to Human Resources SARs mailbox ~ SARs Manchester SARsManchester@rbs.co.uk.

You can make changes to your personal information where it is incorrect or delete your personal information via self-service on Workday or by contacting Colleague Services if you legitimately think that the bank shouldn’t be processing that personal information, is processing it incorrectly or the information is incomplete or inaccurate. Please note that there may be circumstances where you request us to block or restrict our processing of your personal information or to delete it, but we are legally entitled to continue processing your personal information and / or to refuse that request, or are obliged to retain it. If access, correction or deletion is denied, the reason for the denial will be communicated to you.

It is your responsibility to keep your personal information up to date on the Personal Information section of Workday so that accurate records can be maintained.

Inquiries, objections and complaints

Where we rely on your consent to processing your personal information you have the right to withdraw your consent to processing of your personal information at any time. Please note, however, that we may still be entitled to process your personal information if we have another legitimate reason (other than consent) for doing so.

If you have any queries about this Notice or your personal information generally, including questions about accessing your personal information or correcting it, you should contact Colleague Services.

You have the right to lodge a complaint with the data protection regulator if you think that any of your rights have been infringed by us. You can find out more information about your rights by contacting the applicable data protection regulator (Schedule 2).

Automated processing

We do not generally make decisions based solely on automated decision-making within the meaning of the EU General Data Protection Regulation (“GDPR”). In the event that the bank relies solely on automated decision-making that could have a significant impact on you, we will provide you an opportunity to express your views and will provide any other safeguards required by law.

Anti-Commodification Clause

The Bank commits that it will not turn worker data into a commodity for sale or trade.

Respect and Human Rights

The Bank is committed to respecting your privacy and human rights as defined in law and in particular with regard to the UN's Universal Declaration of Human Rights and the ILO's 1997 Code of Practice on the Protection of Workers Personal Data.

Changes to this Privacy Notice

We may make changes to this Privacy Notice from time to time and will inform you when the Privacy Notice is updated. Current versions will be posted on the Temporary, Agency & Contractor pages on the Intranet.

Processing Conditions

The bank's entitlement to process your personal information is governed by a number of processing conditions. This means that we will rely on more than one of these conditions in order to process elements of your personal information during and after your assignment.

a) The bank will also process your personal information where it is required by law or regulation, for example health and safety laws, employment or tax laws, equalities laws and laws and regulations intended to prevent and detect crime and meet the regulatory requirements of the Prudential Regulatory Authority and the Financial Conduct Authority Conduct Rules;

b) The bank will process your personal information where it is in the legitimate interests of the worker or the bank. This processing will always be fair and lawful and will at all times comply with the principles of applicable privacy laws in the country where you are employed;

c) During the course of your assignment it may also be necessary for the bank or its suppliers to process your special categories of information (including information about criminal convictions or offences) as per the detail in Schedule 1 of this notice. This processing will only be carried out:

   i. where you have provided your explicit consent (which may be captured where you provide special categories of information to the bank and its suppliers or affiliates); or

   ii. where it necessary to prevent or detect unlawful acts, fraud or money laundering; or

   iii. in connection with any actual or prospective legal proceedings, for obtaining legal advice, or for establishing, exercising or defending our or your legal right

Schedule 1: Full list of information we may process

- Name, work and home contact details
- Gender and date of birth
- Education and work history
- Emergency contacts' details
- Staff number, job title, grade and job history
- Engagement relationship related information (including compensation, location, hours of work and so on)
- Reporting and managerial relationships
- Photograph(s)
- Time and attendance details
- Expenses such as travel
- Skills and qualifications
- Training history and plans
- Company property assigned (such as laptop, mobile device and so on)
- Technology security/access permissions, log in details and profiles
- Results of original and ongoing worker screening, where relevant (see section 5)
- Use of company equipment and IT systems, including communication resources such as phones, emails etc.
- Details provided in relation to Conduct policies (such as conflicts of interest, personal account dealing, trade body membership and so on)
- *Health & safety incidents, accidents at work and associated records
- Building CCTV images
- Audio recordings of interactions with customers

* These categories of information might potentially include some special categories of information. Special categories of information are not routinely collected about all workers but may be collected where the bank has a legal obligation to do so, or if you choose to disclose it to us during the course of your relationship with the bank.

Schedule 2: Regulator Website

UK	https://ico.org.uk/
Republic of Ireland	https://www.dataprotection.ie/docs/Home/4.htm