Employee Privacy Notice (UK, ROI, Channel Islands, Gibraltar and Isle of Man)

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

Last update: October 2020

Employee Privacy Notice (UK, ROI, Channel Islands, Gibraltar and Isle of Man)

As your employer and a member of the NatWest Group (the "bank", "we," "us," and "our"), the bank collects and holds personal and special categories of 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. The data controller of your personal information will be the entity with whom you entered your employment contract.

This Employee 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.

This Privacy Notice replaces the previous data protection policy and any references to the data protection policy in your contract should be read to refer to this Privacy Notice.

Why do we collect your personal information?

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

Employee Management: day-to-day management of your employment relationship with us (like employee engagement and communications; performance development and training; relocation assistance; corporate travel and other reimbursable expenses; obtaining and maintaining insurance; sickness and absence recording; auditing, assurance and risk management activities; conflict of interest reporting; disciplinary or grievance procedures; and other general administrative operations in connection with your employment with us);

Pay and benefits: to pay you and provide you with the benefits to which you are entitled (like sick pay, maternity pay and pensions) and as necessary to comply with our legal obligations to Her Majesty's Revenue & Customs ("HMRC"), the Irish Revenue Commissioners or other government bodies with regards to taxation;

Share Schemes and Incentive Awards: in connection with any invitation, potential participation and participation in share awards and incentives schemes, including where required to administer those schemes and to comply with our legal obligations;

Workforce Organisation & Strategy: where necessary to analyse and produce reports on our workforce, consider future strategy, to undertake succession planning; 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 by facilitating access to and monitoring activity on and in our premises and activity using our computers, devices, networks, communications and other assets and resources. See section 0) for more information on employee monitoring;

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

Marketing: to inform you about the bank and its partners' products and services that might be relevant to you, such as products with preferential rates for employees. This will only happen if you have agreed to us contacting you in this way;

Pre-Employment Screening: to carry out financial, credit and insurance risk assessments; performing criminal records checks, adverse media checks, screening against external databases and sanctions lists and establishing connections to politically exposed persons;

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

Equality of Opportunity: to ensure equality of opportunity and treatment in compliance with policy and equal opportunities legislation;

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 regarding individual employees and for regulatory submissions.

Business Activities: peripheral processing of your personal information in the course of providing products/services to our customers, responding to customers' inquiries related to these products/services and to contacting customers when reasonably required.

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. 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 and place of birth, nationality (including copies of passports), national insurance number, personal email addresses and phone numbers;
- Education and work history including qualifications, skills and references;
- Emergency contacts' and beneficiaries' details;
- Correspondence with or about you, for example letters to you about a pay rise or, at your request, a letter to your mortgage company confirming your salary;
- Work related information such as employee ID, RACF ID, job title, objectives, managers, attendance and absence records, disciplinary or grievance details and accident records;
- Photographs and images from CCTV;
- Financial information such as salary and expenses and bank account details;
- Information about your shareholdings for the purposes of personal account dealing in shares, including the names and details of persons closely associated with you;
- Information about the benefits you receive including partner and dependant details; and
- Access details for premises (including NIACs data) and IT and details of any bank owned property you hold.

Your Special Categories of Information

Where necessary we may process special categories of information relating to your racial or ethnic origin, religious of philosophical beliefs, trade union membership, physical or mental health or condition, sexual orientation, as well as biometric data for identification purposes. We may also process data relating to criminal convictions and offences. We will only process special categories of information or criminal convictions and offences data where we have obtained your explicit consent or as otherwise permitted by applicable laws. Where we are processing personal information based on your consent, you have the right to withdraw that consent at any time.

For example:

- With your explicit consent we may process information about your sexual orientation or ethnic origin in order to monitor workplace diversity;
- In compliance with our legal obligations under equal opportunities legislation, health and safety and occupational health we may process information about your physical or mental health or condition, sexual orientation or ethnic orientation; and

- In order to administer and manage statutory and company sick pay we may process information about your physical or mental health or condition in order to monitor attendance and absence, and in order to ensure you receive the correct entitlements or support.

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 European Economic Area ("EEA").

Where we transfer your personal information outside the 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 EEA. 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 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 or the provision of employee benefits).

Internally your personal information may be shared with the following people. Access to employee 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 or structure charts);
- Those employees with managerial responsibility for you;
- Employees in HR who have responsibility for certain HR processes (for example compensation, grievance, disciplinary, performance 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 employees 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:

- Purchasers and potential purchasers of the bank's businesses, including joint venture partners;

- 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;
- Third-party suppliers (or potential suppliers), who provide services on our behalf;
- Third parties that administer your benefits, including pension funds and share scheme administrators, employee benefit trustees, any nominee holding shares on your behalf and any broker arranging the sale of shares on your behalf; and
- Professional advisors.

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 our employees and 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 and development feedback.

What kind of activity and information will be monitored?

- Emails and instant messages sent, received and archived on bank provided mobile and PC 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;
- Internet chatroom usage (such as Bloomberg and Reuters) and usage access via bank networks or devices;
- All information stored or processed on your bank computer which may include (but is not limited to) your PC, laptop, mobile phone, tablet or 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.

Screening checks and regulatory reporting

During your employment, we may undertake certain checks as set out below. If you are a member of staff who falls within the scope of the Approved Persons, Certification or Senior Managers Regime then a combination of these checks may be utilised to evidence the bank's compliance with fitness and propriety requirements. We may also need to disclose your personal information to the bank's regulators in order to satisfy our reporting obligations.

Criminal records checks

Given the nature of our business, we have legal and regulatory obligations to ensure that the people we employ can be relied upon to handle client money and information responsibly. We may therefore ask questions about any prior civil or criminal proceedings you may have been subject to and may also conduct criminal record checks.

Credit reference agencies

Similarly, depending on the role you undertake and in which country, we may undertake searches about you through credit reference agencies who will supply us with information in support of our recruitment decision. The agencies will record details of the search but will not make them available for use by lenders to assess your ability to obtain credit. Credit reference checks will not be carried out where these are prohibited by local law.

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 employment 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. We are not able to employ anyone on a 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.

Regulatory reporting

In the event that the bank takes disciplinary action (including Accountability decisions) against you in connection with conduct that constitutes a breach of the Conduct Rules (as set out in Our Code), we may be required to report details of the matter to our regulators. Any such reporting will be carried out in accordance with our internal policies and local laws and will contain the personal information which the regulators have mandated us to provide.

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 the HR Portal or by contacting HR People 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 My Information section of the HR homepage so that accurate employment 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 HR People 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 employee 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.

Direct Marketing

We may use your personal information to inform you about the bank and its partners' products and services that might be relevant to you, such as products with preferential rates for employees ("direct marketing"). This will only happen where you indicated to us via your marketing preferences that you wish to be contacted in this way or provide your personal information to third parties for their direct marketing. You have the right to object to direct marketing.

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 Human Resources Portal.

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 employment.

a) The bank will process your personal information where it is necessary for the performance of our contract with you, for example in the administration of your employee or pensioner

relationship, in order to provide elected or entitled benefits or awards, and in order to fulfil the legal obligations created within your employment contract;

b) 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;

c) The bank will process your personal information where it is in the legitimate interests of the employee 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;

d) During the course of your employment 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 section 2 and Schedule 1 of this notice. This processing will only be carried out:

   i. on the basis of 8(a) and 8(b) above; or

   ii. 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

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

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

Schedule 1: Full list of information we may process

- Name, work and home contact details
- Date and place of birth
- Education and work history
- *Individual demographic information in compliance with legal requirements (such as marital status, national identifier, passport/visa information, nationality, citizenship, military service, disability, work permit, date and place of birth or gender)
- Emergency contacts' and beneficiaries' details
- *Information relating to individual's partners and dependants (such as name, age) for determination of benefit eligibility
- *Health issues requiring adaptations to working environment
- Staff number, job title, grade and job history
- Goals, objectives, mid-year and end of year reviews
- Employment contract related information (including compensation, location, hours of work and so on)
- Reporting and managerial relationships
- *Leaves of absence (such as maternity leave, sickness absence)
- Photograph(s)
- Termination details for ex-employees (like reason for leaving)
- Disciplinary / grievance records
- Travel bookings
- Time and attendance details
- *Deductions to be taken from individual pay
- *Bank account details for salary payment purposes
- Bonus payments, compensation data and benefits and entitlements data
- Share scheme membership details and personal information connected to share scheme participation (e.g. social security number, national insurance number, executor's names, power of attorney names, court appointed official names, bankruptcy/court order status, work email address and details of any shares of common stock or directorships)

- Expenses (including corporate credit card transactions) such as travel and living expenses claimed from the bank
- Skills and qualifications
- Training history and plans
- Company property assigned (such as laptop, BlackBerry, car and so on)
- Technology security/access permissions, log in details and profiles
- Results of original and ongoing employee screening, where relevant (see section 5)
- Use of company equipment and IT systems, including communication resources such as phones, emails etc. (see section 0
- 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 employee interactions with customers
- Individual direct marketing preferences

* These categories of information might potentially include some special categories of information. Special categories of information are not routinely collected about all employees, 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 Websites

UK	https://ico.org.uk/
Gibraltar	http://www.gra.gi/data-protection
Guernsey	https://dataci.gg/
Isle of Man	https://www.inforights.im/
Jersey	https://oicjersey.org/
Republic of Ireland	https://www.dataprotection.ie/docs/Home/4.htm