

Savings Privacy Notice

Your personal information and what we do with it



With effect from 10th May 2024.

WHO WE ARE AND HOW TO CONTACT US AND OUR DATA PROTECTION OFFICER

Newbury Building Society of 90 Bartholomew Street, Newbury, RG14 5EE is a data controller of your personal information. This means information that is about you or from which we can identify you. This privacy notice describes how we deal with your personal information. We are the data controller of this information under relevant data protection laws because in the context of our business relationship with you we decide how and why it is processed in the ways explained in this privacy notice. When we use terms such as **we**, **us** and **our** in this notice, we mean Newbury Building Society.

Our Data Protection Officer can be contacted if you have queries about this privacy notice or wish to exercise any of the rights mentioned in it. You can contact our Data Protection Officer by writing to Newbury Building Society, 90 Bartholomew Street, Newbury, RG14 5EE or via our website at www.newbury.co.uk/contact/.

You will see at the end of this privacy notice that we mention the privacy notice of Credit Reference Agencies ("CRAs"). We need to share this with you. Please read it carefully and contact those organisations if you have questions (their details are in their notices). We also explain in this notice why we use Credit Reference Agencies.

This privacy notice may be updated from time to time. If we are going to use your personal data for any new purposes, we will bring any changes to the privacy notice to your attention. The latest version of the Society's privacy notice is available via our website at www.newbury.co.uk/privacy-notice/, in any of our branches or by calling us on 01635 555700.

PERSONAL INFORMATION THAT WE PROCESS IN CONNECTION WITH A SAVINGS PRODUCT

We use many different kinds of personal information, and group them together like this.

Category of personal information	Description
Identification	Your title, full name, date of birth and/or age, e.g. to make sure that you are eligible to apply for the product and/or that it is suitable for you.
Financial	Your financial details e.g. details of your savings, source of your wealth and funds, information about your tax position and details of account(s) held with other providers if you pay out of or into your savings account to or from those other account(s).
Residence	Your home address, correspondence address (where different from your home address), your address history, information which is relevant for your residency and/or citizenship status, such as your nationality and your place of birth, if this is necessary for us to comply with our legal and regulatory requirements.
Contact	Your contact details including for instance your email address, home and mobile telephone numbers.
Transactional	Details about payments to and from your accounts with us. Where a person other than the savings account holder makes a withdrawal from the account, information about that person and the transaction.
Contractual	Details about the products or services we provide to you.
Behavioural	Details about how you use our products and services.
Communications	Records of how you have contacted us, for example letters, emails, and conversations between us.
Documentary Data	Details about you that are stored in documents in different formats, or copies of them. This could include things like your passport, drivers licence, or birth certificate.
Special types of data	Some special categories of personal data such as about your health or if you are a vulnerable customer (more details below).
Consents	Any permissions, consents, or preferences that you give us. This includes things like how you want us to contact you and whether you wish to receive marketing information.
Fraud Prevention	Personal information which we obtain from Fraud Prevention Agencies (see the section on 'Fraud Prevention Agencies' below).

JOINT APPLICANT AND POWERS OF ATTORNEY

If you make a joint application with your spouse, partner or family member, we will also collect the personal information mentioned above about that person. You must show this privacy notice to the other applicant and ensure they confirm that they know you will share their data with us for the purposes described in it. If you look at the “What are the legal grounds” section (below) you will see reference to consent and a description of some limited scenarios where it may be relevant to what we do with personal information. If we ask you to obtain consent from the joint applicant (such as for marketing) you should do that using the consent section that we give or make available to you for that purpose.

If there is somebody who has power of attorney over your affairs, that person will see this privacy notice when we make contact with them directly.

WHAT IS THE SOURCE OF YOUR PERSONAL INFORMATION?

We will generally collect your personal information from you directly.

In addition, we obtain your personal information from other sources such as Fraud Prevention Agencies, Credit Reference Agencies, social media, internet, news articles, other organisations to assist in prevention and detection of crime, police and law enforcement agencies.

Some of the personal information obtained from Credit Reference Agencies will have originated from publicly accessible sources. In particular, Credit Reference Agencies draw on court decisions, bankruptcy registers and the electoral register (also known as the electoral roll). We explain more about Credit Reference Agencies below.

WHAT ARE THE LEGAL GROUNDS FOR OUR PROCESSING OF YOUR PERSONAL INFORMATION (INCLUDING WHEN WE SHARE IT WITH OTHERS)?

Data protection laws require us to explain what legal grounds justify our processing of your personal information (this includes sharing it with other organisations). For some processing more than one legal ground may be relevant (except where we rely on consent). Here are the legal grounds that are relevant to us:

1. Processing necessary **to perform our contract with you for the savings product or for taking steps prior to entering into it (during the application stage)**:
 - a) Administering and managing your savings account and services relating to that, updating your records, tracing your whereabouts to contact you about your account;
 - b) Sharing your personal information with other payment services providers such as when you ask us to share information about your account with them;
 - c) All stages and activities relevant to managing your savings account including enquiry, application, administration and management of accounts, illustrations; and
 - d) For some of our profiling and other automated decision making which are described later in this notice.
2. Where we consider that, on balance, it is appropriate for us do so, processing necessary **for the following legitimate interests** which apply to us are:
 - a) To test the performance of our products, services and internal processes;
 - b) To adhere to guidance and best practice under the regimes of governmental and regulatory bodies such as HMRC, the Financial Conduct Authority, the Prudential Regulation Authority, the Payment Systems Regulator, the Financial Ombudsman Service, the Information Commissioner’s Office and under the Financial Services Compensation Scheme;
 - c) For management and audit of our business operations including accounting;
 - d) To carry out searches at Credit Reference Agencies pre-application, at the application stage, and periodically after that;
 - e) To carry out monitoring and to keep records (see below);
 - f) To administer our good governance requirements such as internal reporting and compliance obligations or administration required for Annual General Meeting (AGM) processes such as providing you with the notice of AGM, proxy voting form and Members’ Review;
 - g) For market research and analysis and developing statistics;
 - h) For generic member marketing communications to include news stories about us and our members, local events and information about our products and services;
 - i) For some of our profiling and other automated decision making, in particular where this does not have a legal effect or otherwise significantly affect you; and
 - j) When we share your personal information with the other people or organisations listed below:
 - Joint account holders, trustees and beneficiaries and any person with power of attorney over your affairs (in each case only if relevant to you);
 - Other payment services providers such as when you ask us to share information about your account with them;
 - Other account holders or individuals when we have to provide your information to them because some money paid to you by them should not be in your account;
 - People you receive payments from in order to verify the name of the account holder;
 - Other payment service providers you make payments to in order to verify the name of the account holder;
 - Our legal and other professional advisers and auditors;
 - Financial institutions and trade associations;
 - Governmental and regulatory bodies such as HMRC (including for onward transfer to overseas tax authorities), the Financial Conduct Authority, the Prudential Regulation Authority, the Payment Systems Regulator, the Financial Ombudsman Service, the Information Commissioner’s Office and under the Financial Services Compensation Scheme;
 - Other organisations and businesses who provide services to us such as back up and server hosting providers, IT software and maintenance providers, document storage providers and suppliers of other back office functions;
 - Buyers and their professional representatives as part of any restructuring or sale of our business or assets;
 - Credit Reference Agencies (see below where we explain more and refer to a separate leaflet for more information); and
 - Market research organisations that help us to develop and improve our products and services.

3. Processing necessary **to comply with our legal obligations:**
- a) For compliance with laws that apply to us;
 - b) For establishment, defence and enforcement of our legal rights;
 - c) For activities relating to the prevention, detection and investigation of crime;
 - d) To carry out identity checks, anti-money laundering checks, and checks with Fraud Prevention Agencies pre-application, at the application stage, and periodically after that;
 - e) To carry out monitoring and to keep records (see below);
 - f) To deal with requests from you to exercise your rights under data protection laws;
 - g) To process information about a crime or offence and proceedings related to that (in practice this will be relevant if we know or suspect fraud); and
 - h) When we share your personal information with these other people or organisations:
 - Joint account holders, trustees and beneficiaries, and the person with power of attorney over your affairs;
 - Other payment services providers such as when you ask us to share information about your account with them;
 - Other account holders or individuals when we have to provide your information to them because some money paid to you by them should not be in your account;
 - Fraud Prevention Agencies;
 - Law enforcement agencies and governmental and regulatory bodies such as HMRC, the Financial Conduct Authority, the Prudential Regulation Authority, the Payment Systems Regulator, the Ombudsman, the Information Commissioner's Office and under the Financial Services Compensation Scheme (depending on the circumstances of the sharing); and
 - Courts and to other organisations where that is necessary for the administration of justice, to protect vital interests and to protect the security or integrity of our business operations.
4. Processing with your **consent:**
- a) When you request that we share your personal information with someone else and consent to that;
 - b) For direct marketing communications; and
 - c) For some of our processing of special categories of personal data such as about your health or if you are a vulnerable customer (and it will be explained to you when we ask for that explicit consent what purposes, sharing and use it is for).
5. Processing for a **substantial public interest** under laws that apply to us where this helps us to meet our broader social obligations such as:
- a) Processing of your special categories of personal data such as about your health or if you are a vulnerable customer;
 - b) Processing that we need to do to fulfil our legal obligations and regulatory requirements; and
 - c) When we share your personal information with other people and organisations if they need to know that you are a vulnerable customer and your relatives, social services, your carer or the person who has power of attorney over your affairs.

HOW AND WHEN CAN YOU WITHDRAW YOUR CONSENT?

Much of what we do with your personal information is not based on your consent, instead it is based on other legal grounds. For processing that is based on your consent, you have the right to take back that consent for future processing at any time. You can do this by contacting us; details of how to contact us are covered earlier in this notice. The consequence might be that we cannot send you some marketing communications or that we cannot take into account special categories of personal data such as about your health or if you are a vulnerable customer (but these outcomes will be relevant only in cases where we rely on explicit consent for this).

To comply with payment services regulations we have to share some of your personal information with other payment service providers in some circumstances such as when you ask us to share information about your account with them. Whilst those payment services regulations mention 'consent' for this, 'consent' in that context does not have the same meaning as 'consent' under data protection laws. The legal grounds which may be relevant to this are compliance with our legal obligations, performance of our contract with you, our legitimate interests, or a combination of these. This is why if you ask to withdraw consent from what we do with your personal information where we need to have it under the payment services regulations, we may still have to hold and use your personal information.

IS YOUR PERSONAL INFORMATION TRANSFERRED OUTSIDE THE UK?

We are based in the UK but sometimes your personal information may be transferred outside the UK. Some countries outside the UK have adequate protection for personal information under laws that apply to us. We will make sure that suitable safeguards are in place before we transfer your personal information to countries outside the UK which do not have adequate protection under laws that apply to us.

Safeguards include contractual obligations imposed on the recipients of your personal information. Those obligations require the recipient to protect your personal information to the standard required in the UK. Safeguards also include requiring the recipient to subscribe to 'international frameworks' intended to enable secure data sharing and where the framework is the means of protection for the personal information.

HOW DO WE SHARE YOUR INFORMATION WITH CREDIT REFERENCE AGENCIES?

In order to process your application, we will perform identity checks on you with one or more credit reference agencies. Where you take banking services from us, we may also make periodic searches at CRAs to manage your account with us. To do this, we will supply your personal information to CRAs and they will give us information about you. CRAs will supply to us both public (including the electoral register) and fraud prevention information.

We will use this information to:

- Verify the accuracy of the data you have provided to us;
- Prevent criminal activity, fraud and money laundering;
- Manage your account(s); and
- Ensure any offers provided to you are appropriate to your circumstances.

If you are making a joint application, or tell us that you have a spouse or financial associate, we will link your records together, so you should make sure you discuss this with them, and share with them this information, before lodging the application. CRAs will also link your records together and these links will remain on your and their files until such time as you or your partner successfully files for a disassociation with the CRAs to break that link.

The identities of the CRAs, their role also as fraud prevention agencies, the data they hold, the ways in which they use and share personal information, data retention periods and your data protection rights with the CRAs are explained in more detail in the separate leaflet which we refer to later on in this privacy notice.

HOW DO WE SHARE YOUR INFORMATION WITH FRAUD PREVENTION AGENCIES?

This is explained in the separate notice which is included in the section below headed “Fair Processing Notice for the Purpose of Fraud Prevention and Detection”

WHAT SHOULD YOU DO IF YOUR PERSONAL INFORMATION CHANGES?

You should tell us without delay so that we can update our records. You can do so by visiting any of our branches, writing to Newbury Building Society, 90 Bartholomew Street, Newbury, RG14 5EE or via our website at www.newbury.co.uk/contact/.

DO YOU HAVE TO PROVIDE YOUR PERSONAL INFORMATION TO US?

We are unable to provide you with the savings product or to process your application without having personal information about you. Your personal information is required before you can enter into the relevant contract with us, or it is required during the life of that contract, or it is required by laws that apply to us. If we already hold some of the personal information that we need – for instance if you are already a customer – we may not need to collect it again when you make your application.

In cases where providing some personal information is optional, we will make this clear. For instance we will say in application forms, in branch or on our website if sections (such as work telephone number contact details) can be left blank.

DO WE DO ANY MONITORING INVOLVING PROCESSING OF YOUR PERSONAL INFORMATION?

In this section monitoring means any listening to, recording of, viewing of, intercepting of, or taking and keeping records (as the case may be) of calls, email, text messages and social media messages in person, or at a distance.

We may monitor where permitted by law and we will do this where the law requires it. In particular, where we are required by the Financial Conduct Authority’s regulatory regime to record certain telephone lines or in person meetings (as relevant) we will do so.

Some of our monitoring may be to comply with regulatory rules, self-regulatory practices or procedures relevant to our business, to prevent or detect crime, in the interests of protecting the security of our communications systems and procedures, to have a record of what we have discussed with you and actions agreed with you, to protect you and to provide security for you (such as in relation to fraud risks on your account) and for quality control and staff training purposes.

Some of our monitoring may check for obscene or profane content in communications.

We may conduct carefully controlled monitoring of your activities on your savings account where this is necessary for our legitimate interests or to comply with our legal obligations. For instance, where we suspect fraud, money laundering or other crimes.

Telephone calls and/or in person meetings between us and you in connection with your application and the savings product may be recorded to make sure that we have a record of what has been discussed and what your instructions are. We may also record these types of calls for quality control and staff training purposes.

PROFILING AND OTHER AUTOMATED DECISION MAKING

This section is relevant where we make decisions about you using only technology, and where none of our employees or any other individuals have been involved in the process e.g. in relation to transactions on your savings account, payments into your savings account from other providers and triggers and events such as account opening anniversaries and maturity dates. We may do this to decide what marketing communications are suitable for you and to analyse statistics.

We can do this activity based on our legitimate interests (and they are listed in the section about legal grounds above) only where the profiling and other automated decision making does not have a legal or other significant effect on you. In all other cases, we can do this activity only where it is necessary for entering into or performing the relevant contract, is authorised by laws that apply to us, or is based on your explicit consent. In those cases you have the right to obtain human intervention to contest the decision (see ‘rights in relation to automated decision making which has a legal effect or otherwise significantly affects you’ below). Profiling for direct marketing can mean there is a separate right to object (see ‘rights to object’ below).

FOR HOW LONG IS YOUR PERSONAL INFORMATION RETAINED BY US?

Unless we explain otherwise to you, we will hold your personal information for the following periods:

- **Retention in case of queries.** We will retain the personal information that we need to keep in case of queries from you (for instance, if you apply unsuccessfully for a product or service) for 1 year and delete it at the earliest opportunity after that time unless we have to keep it for a longer period (see directly below);
- **Retention in accordance with legal and regulatory requirements and in case of claims.** We will retain the personal information that we need to keep, including transaction data and identification documents, even after the relevant contract(s) you have with us has come to an end. We will retain this data for 5 years after the end of your relationship with us and delete it at the earliest opportunity after that time unless we have to keep it for a longer period.

If you would like further information about our data retention practices, contact us at www.newbury.co.uk/contact/.

WHAT ARE YOUR RIGHTS UNDER DATA PROTECTION LAWS?

Here is a list of the rights that all individuals have under data protection laws. They do not apply in all circumstances. If you wish to exercise any of them we will explain at that time if they apply or not. The right of data portability is only relevant from May 2018.

- The **right to be informed** – we have to be transparent with you about the processing that we do with your personal information. This is why we have a privacy notice. The information that you supply is determined by whether or not we collected your personal information directly from you or indirectly via someone else. Your right to be informed may be relevant if you consider it necessary to ask for more information about what we do with your personal information.
- The right to have your personal information **corrected if it is inaccurate** and to have **incomplete personal information completed** in certain circumstances. If we have disclosed the personal information in question to other organisations, we must inform them of the rectification where possible. Your rights in relation to rectification may be relevant if you consider that we are processing inaccurate or incomplete information about you.
- The **right to object** to processing of your personal information where it is based on legitimate interests, where it is processed for direct marketing (including profiling relevant to direct marketing) or where it is processed for the purposes of statistics. Your rights to object may be relevant if you wish to find out more about what legitimate interests we rely on (they are listed in our privacy notice) or about what profiling we do in relation to our direct marketing communications and activities (as mentioned in our privacy notice) for instance. There is an important difference between the right to object to profiling relevant to direct marketing in cases where that profiling activity does not have a legal effect on you or otherwise significantly affect you, and the separate right which exists under data protection laws in relation to profiling including automated decision making which has a legal effect or can otherwise significantly affect you (see below).
- The **right to restrict processing** of your personal information, for instance where you contest it as being inaccurate (until the accuracy is verified); where you have objected to the processing (where it was necessary for legitimate interests) and we are considering whether our organisation's legitimate interests override your own; where you consider that the processing is unlawful (and where this the case) and where you oppose erasure and request restriction instead; or where we no longer need the personal information for the purposes of the processing for which we were holding it but where you require us to continue to hold it for the establishment, exercise or defence of legal claims.
- The **right to have your personal information erased** (also known as the "right to be forgotten"). This enables an individual to request the deletion or removal of personal information where there is no compelling reason for its continued processing. This right is not absolute – it applies only in particular circumstances and where it does not apply any request for erasure will be rejected. It may be relevant where the personal information is no longer necessary in relation to the purpose for which it was originally collected/processed; if the processing is based on consent which you then withdraw; when you object to the processing and there is no overriding legitimate interest for continuing it; if the personal information is unlawfully processed; or if the personal information has to be erased to comply with a legal obligation. Requests for erasure may be refused in some circumstances such as where the personal information has to be retained to comply with a legal obligation or to exercise or defend legal claims.
- The **right to request access** to the personal information held about you, to obtain confirmation that it is being processed, and to obtain certain prescribed information about how we process it. This may assist if you wish to find out what personal information we do have about you in order to then determine if you can exercise other rights (those mentioned above and below).
- The **right to data portability**. This allows individuals to obtain and reuse their personal information for their own purposes across different services; to move, copy or transfer their personal information easily from one environment to another in a safe and secure way without hindrance to usability. This right can only be relevant where personal information is being processed based on a consent or for performance of a contract and is carried out by automated means. This right is different from the right of access (see above) and that the types of information you can obtain under the two separate rights may be different. You are not able to obtain through the data portability right all of the personal information that you can obtain through the right of access.
- Rights in relation to **automated decision making which has a legal effect or otherwise significantly affects you**. This right allows individuals in certain circumstances to access certain safeguards against the risk that a potentially damaging decision is taken solely without human intervention. This right is different from the more general right to object to profiling (see above) because that other right is not tied to a scenario where there is a legal effect on you or where the processing otherwise significantly affects you. Data protection laws prohibit this particular type of automated decision making except where it is necessary for entering into or performing a contract; is authorised by law; or where you have explicitly consented to it. In those cases, you have the right to obtain human intervention and an explanation of the decision and you may be able to challenge that decision.

You have the right to complain to the Information Commissioner's Office which enforces data protection laws. You can contact the Information Commissioner's Office at <https://ico.org.uk/>. If you wish to exercise any of these rights against the Credit Reference Agencies or the Fraud Prevention Agencies, you should contact them separately.

DATA ANONYMISATION AND USE OF AGGREGATED INFORMATION

Your personal information may be converted into statistical or aggregated data which cannot be used to re-identify you. It may then be used to produce statistical research and reports. This aggregated data may be shared and used in all the ways described in this privacy notice.

YOUR MARKETING PREFERENCES AND WHAT THIS MEANS

We may use your home address, phone numbers, email address and social media (e.g. Facebook, Twitter, Google and message facilities in other platforms) to contact you according to your marketing preferences. This means we do this only if we have a legal ground which allows it under data protection laws – see above for what is our legal ground for marketing.

If you wish to stop receiving communications from us, you will be able to do so at any time by:

- emailing marketing@newbury.co.uk;
- visiting our marketing preferences page through the links available in our emails and website footer;
- calling us on 01635 555700;
- visiting any of the Society's branches;
- post to Newbury Building Society, 90 Bartholomew Street, Newbury, RG14 5EE;
- following the unsubscribe link contained in our email communications.

DATA PRIVACY NOTICES FROM OTHER ORGANISATIONS

We have mentioned that we share your personal information with Fraud Prevention Agencies and Credit Reference Agencies. They require us to pass on to you information about how they will use your personal information to perform their services or functions as data controllers in their own right. These notices are separate to our own. The Credit Reference Agency Information Notice is in a separate leaflet which is available via our website at www.newbury.co.uk/privacy-notice/, in any of our branches or by calling us on 01635 555700. The Fraud Prevention Agency fair processing notice is detailed in the next section.

FAIR PROCESSING NOTICE FOR THE PURPOSE OF FRAUD PREVENTION AND DETECTION

General

1. Before we provide services, goods or financing to you, we undertake checks for the purposes of preventing fraud and money laundering, and to verify your identity. These checks require us to process personal data about you.
2. The personal data you have provided, we have collected from you, or we have received from third parties will be used to prevent fraud and money laundering, and to verify your identity.
3. Details of the personal information that will be processed include, for example: name, address, date of birth, contact details, financial information and employment details.
4. We and fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.
5. We process your personal data on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us. Such processing is also a contractual requirement of the services or financing you have requested.
6. 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.

Consequences of processing

7. If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services or financing you have requested, or to employ you, or we may stop providing existing services to you.
8. A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services, financing or employment to you. If you have any questions about this, please contact us on the details above.

Data transfers

9. Fraud prevention agencies may allow the transfer of your personal data outside of the UK. This may be to a country where the UK Government has decided that your data will be protected to UK standards, but if the transfer is to another type of country, then the fraud prevention agencies will ensure your data continues to be protected by ensuring appropriate safeguards are in place.

Your rights

10. Your personal data is protected by legal rights, which include your rights to object to our processing of your personal data; request that your personal data is erased or corrected; request access to your personal data.
11. For more information or to exercise your data protection rights, please contact us using the contact details above.
12. You also have a right to complain to the Information Commissioner's Office which regulates the processing of personal data.

GLOSSARY

Automated decision making means a process where we make decisions about you, such as your suitability for a product, using a computer based and automated system without a person being involved in making that decision.

Profiling means any form of automated processing of your personal information to evaluate certain personal aspects about you, such as to analyse or predict aspects concerning your economic situation, health, personal preferences, interests, reliability or behaviour.

Process or processing includes everything we do with your personal information from its collection, right through to its destruction or deletion when we no longer need it. This includes for instance collecting it (from you), obtaining it (from other organisations), using, sharing, storing, retaining, deleting, destroying, transferring it overseas.

Legitimate interests is mentioned in our privacy notice because data protection laws allow the processing of personal information where the purpose is legitimate and is not outweighed by your interests, fundamental rights and freedoms. Those laws call this the legitimate interests legal ground for personal data processing.

Payment services providers means the institution you use to make payments on your behalf, for example your bank.