OUR PRIVACY NOTICE

The Nottingham For Intermediaries

1. ABOUT THE NOTTINGHAM

We're The Nottingham, a group of companies that includes Nottingham Building Society. The Nottingham is the controller for the personal information we use, unless otherwise stated. Wherever you see "we," "us" or "our" it means The Nottingham.

2. INTRODUCTION

This Privacy Notice tells you what to expect us to do with your personal information when you use our products or services. It also outlines the steps we take to ensure that your personal data is protected and describes the rights you have in relation to the data we use.

3. OUR DATA PROTECTION OFFICER

If you have any questions about this Notice, please don't hesitate to contact our Data Protection Officer:

- by e-mail: dpo.dpo@thenottingham.com
- by post: Data Protection Officer, Nottingham Building Society, Nottingham House, 3 Fulforth Street, Nottingham, NG1 3DL

4. WHAT INFORMATION DO WE COLLECT?

We obtain your information from a range of sources; some of it will come directly from you or someone else you've asked us to obtain information from. We might also get some of it from third parties and from publicly accessible sources. This might include:

- Name, previous names, address, date of birth, place of birth, gender and contact information (for example, postal address, e-mail address and telephone numbers)
- Information about your work or profession, your nationality, education, social and economic demographic
- Information we need to enable us to check your identity, process an application and complete credit referencing (for example photo identification, passport information, national insurance number and nationality)
- Information for accounts you hold with us including payments and withdrawals, services you use, and other related information
- Information we need to be able to process payments for you, for example bank and credit or debit card details
- Information and opinions given if you take part in market research
- User login and subscription details (for example, login credentials for mobile apps)
- Information collected through cookies and other technologies we use to recognise you, remember your preferences, and tailor the content we provide to you – our cookies policy provides more details
- Information about your device or the software you use (for example, its ip address, technical specification and uniquely identifying data)
- Geographic information such as which branches you use
- Information about your financial position and history, which may include source of funds and wealth
- Information relevant to your marketing preferences
- Records of contact we have had with you, such as e-mails, system notes and letters
- information you've asked us to collect for you (for example, details about your accounts with us or other companies including transaction data)
- CCTV images and recordings in our branches
- Details about your health and lifestyle (for example, in order to provide you with an insurance policy or if you require extra support due to a health condition or other vulnerability)
- Information about criminal convictions and offences (for example, if relevant for mortgage applications)
- Information about your race or national or ethnic origin.

If you do not provide information that we tell you is mandatory (that is, which you must provide), it may mean that we cannot provide you with the product or service you want or meet all our obligations to you. We sometimes ask for personal information that is useful, but not required by law or a contract. We will make this clear when we ask for it. You don't have to give us these extra details, and it won't affect the products or services you have with us.

5. HOW WE PROTECT YOUR INFORMATION

The security of your information is very important to us. We maintain physical, electronic, and procedural safeguards in relation to the collection, storage, and disclosure of personal data to prevent unauthorised access, accidental loss, disclosure, or destruction.

6. YOUR DATA PROTECTION RIGHTS AND HOW TO EXERCISE THEM

Under data protection law, you have rights we need to make you aware of. The rights available to you depend on the reason we use your information:

1. You have the right to **access** your personal data. This is commonly referred to as data subject access. You can make a data subject access request verbally or in writing. We have one month to respond to a request and cannot charge a fee to deal with a request in most circumstances.
2. You have the right to ask us to **rectify** information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.
3. You may request that we **erase** your personal information if you believe that: we no longer need to use your information for the purposes for which it was provided; we have requested your permission to use your personal information and you wish to withdraw your consent; or we are not using your information in a lawful manner.
4. You have the right to **object** if we are using information based on our legitimate interests. Legitimate interests are when we have a business or commercial reason to use your personal information but our interests must not conflict unfairly with your interests. Please be aware that we can still use information where there are compelling grounds, or it is necessary for us to defend legal claims.
5. You have the right to ask us to **restrict** the use of your information in certain circumstances. You may request to restrict the use of your personal information if you believe that: any of the information that we hold about you is inaccurate; we no longer need to use your information, but you want us to keep it to create, exercise or defend legal claims; we are not using your information in a lawful manner.
6. You have the right to ask that we **transfer** the information you gave us from one organisation to another or give it to you. This right only applies to information you have given us which we are processing information based on your consent. This is known as the right to data portability.

You can withdraw your consent for us to use your personal information at any time (when our reason for using your personal information is that we have your consent). If you withdraw your consent, we may not be able to provide certain products or services to you. If this is so, we will tell you.

For more information about how to exercise your data protection rights, please contact us at datasubjectrights@thenottingham.com or on 0303 123 1113.

7. COMPLAINTS

We work to high standards when it comes to using your personal information. If you have any queries or concerns, please contact us at:

- By e-mail: dpo.dpo@thenottingham.com
- By post: Data Protection Officer, Nottingham Building Society, Nottingham House, 3 Fulforth Street, Nottingham, NG1 3DL.

If you remain dissatisfied, you can make a complaint to the Information Commissioner's Office which regulates the use of personal data, by visiting ico.org.uk/make-a-complaint

8. HOW LONG DO WE KEEP YOUR INFORMATION?

We keep your information in line with our data retention and disposal policies. This enables us to meet our legal and regulatory obligations or use it where we need to for our legitimate purposes such as managing your account and dealing with any disputes or concerns that may arise.

If you would like more information on this, please feel free to contact us by using the contact details provided in this Notice.

9. WHO DO WE SHARE YOUR INFORMATION WITH?

We may share your information where it's lawful to do so. This includes with:

- Companies in the nottingham group and any sub-contractors, agents or service providers who work for us or provide services to us (including their employees, sub-contractors, service providers, directors, and officers)
- Business partners or agents who support us to deliver our products and services to you, or that we refer you to, or that refer you to us
- Any joint account holders, trustees, beneficiaries, or executors
- Anyone who provides instructions or operates any of your accounts on your behalf, for example, power of attorney, solicitors, intermediaries, brokers etc.
- Third parties where you have asked us to share your information
- Third parties where it's necessary to enter into or necessary for the performance of a contract
- People who give guarantees or other security for any amounts you owe us
- People you make payments to and receive payments from
- Other financial institutions, lenders, and holders of security over any property you charge to us, tax authorities, trade associations, payment service providers and debt recovery agents
- Any people or companies in connection with potential or actual corporate restructuring, merger, acquisition, or takeover, including any transfer or potential transfer of any of our rights or duties under our agreement with you
- Organisations that help us to run our annual general meeting (agm)
- Organisations providing essential services to support us in managing our relationship with you and operating our business.
- Credit reference agencies.
- Third-party organisations that conduct research, analysis, and marketing activities on our behalf
- Law enforcement agencies, government, courts, dispute resolution bodies, our regulators, auditors, and any party appointed or asked for by our regulators to carry out investigations or audits of our activities
- Fraud prevention agencies who will also use it to detect and prevent fraud and other financial crime and to confirm your identity
- If our relationship is because of an insurance policy we'll also share your information with other parties involved in providing your insurance policy, for example, the insurer who provides your cover/policy
- The emergency services in exceptional circumstances when we believe it's in your interests, such as in the case of accident or emergency.

When selecting our business partners, we take appropriate steps to make sure that they have adequate protection in place and that they follow data protection legislation.

There are times when we engage third parties which involves them using data on our behalf. We refer to these third parties as processors. When this happens, we ensure that this is done in a way that meets legal requirements and that there is a written contract in place so that both parties understand their responsibilities and liabilities.

10. CREDIT REFERENCE CHECKS, FRAUD AND MONEY LAUNDERING

Credit Reference Checks

If you apply for new products or services, we may carry out credit and identity checks on you with one or more of our trusted partner credit reference agencies (CRAs) and digital identity and screening providers. When you use our banking services, we may also make periodic searches to manage your account with us. To do this, we will supply your personal information to the trusted partners, and they will give us details about you. They will supply us with both public (including the electoral register) and shared credit information, financial situation, history, and fraud prevention information. We may use this information to:

- Assess whether you can afford the product you applied for
- Verify the accuracy of the data you've given us
- Prevent criminal activity, fraud, and money laundering
- Manage your account(s)
- Trace and recover debts
- Ensure any offers provided to you are appropriate to your circumstances
- Personalise and improve our products and services
- Make statistical reports for business purposes

Whilst you have a relationship with us, we will continue to exchange information about you with our trusted partners. We will also inform the CRAs about your repayment history. If you borrow and do not repay in full and on time, CRAs will record the outstanding debt. This information may be supplied to other organisations by CRAs. When CRAs receive a search request from us they will place a marker on your credit file that may be seen by other lenders.

If you're making a joint application or tell us that you have a spouse or financial associate, we'll link your records together. You should discuss this with them and share this information with them before submitting the application.

The identities of the CRAs, digital identity and screening providers, 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 on their websites.

Credit reference agencies:

CRAs have created a joint document called the Credit Reference Agency Information Notice (CRAIN) which is available from each of the three CRAs – going to any of these three links will take you to the same CRAIN document:

- Transunion - transunion.co.uk/crain
- Equifax - equifax.co.uk/crain
- Experian - experian.co.uk/crain

Identity Verification and Screening Providers

Our identity verification and screening partners are listed here. More information may be obtained from their websites:

- Onfido - onfido.com/privacy
- SmartSearch - smartsearch.com/privacy-policy

Consequences of using information in this way

If we, or a fraud prevention agency, have reason to believe there's a fraud or money laundering risk, we may refuse to provide the services and credit you've requested. We may also stop providing existing products and services to you. A record of any fraud or money laundering risk will be kept by the fraud prevention agencies. This may also be used to enhance fraud detection models and may also result in others refusing to provide services to you. The information we hold about you could make it easier or harder for you to get credit in the future.

Fraud prevention agencies

We'll carry out checks with fraud prevention agencies for the purposes of preventing fraud and money laundering, and to confirm your identity before we provide products and services to you.

We, and fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.

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.

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.

To find out more about our Fraud Prevention Agencies and how they manage your information, visit each agency directly:

- CIFAS - cifas.org.uk/fpn
- National Hunter - nhunter.co.uk/privacypolicy
- Synectics Solutions Ltd - synectics-solutions.com/privacy

11. LINKS TO OTHER WEBSITES

Where we provide links to websites of other organisations, this Privacy Notice does not cover how that organisation processes personal information. We encourage you to read the Privacy Notices on the other websites you visit.

12. AUTOMATED PROCESSING

Automated processing means a decision-making process that is automated and excludes any human influence on the outcome. Examples include:

Credit and affordability assessments.

We will consider a number of factors, including information about your income, your outgoings and how well you have kept up on payments in the past. This will be used to work out the amount we could lend you and you could comfortably afford to pay back.

Protecting you and your account against criminal or fraudulent activity

We will assess your transactions to identify any that are unusual. This may stop us from making a payment that is likely to be fraudulent.

Protecting us against criminal or fraudulent activity

We will assess a number of factors such as whether you have provided false information in the past, where you might be at the time and other information about your credit history to decide whether you are a fraud or financial-crime risk (for example, whether offering services to you may break or not be in line with our legal obligations). If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services you have requested, or to employ you, or we may stop providing existing services to 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 provide services, financing, or employment to you. If you have any questions about this, please contact us.

If we are carrying out solely automated decision-making that has legal or similarly significant effects on you, we can only carry out this type of decision-making where the decision is:

- Necessary for us to enter into a contract. For example, we may decide not to offer our services to you based on your credit history and other financial information we have collected about you.
- Required or authorised by law (for example, to prevent financial crime).
- Based on your explicit consent.

You have rights in relation to automated decision making (including profiling where this is part of an automated decision-making process) where the result will have legal or other significant effects on you. You have a right:

- Not to be subject to a decision that is based solely on automated processing if the decision affects your legal rights or other equally important matters (e.g., automatic refusal of an online application). You can object to an automated decision we have made and ask that a person reviews it.
- To understand the reasons behind decisions made about you by automated processing and the possible consequences of the decisions.
- To object to profiling in certain situations, including for direct marketing.

13. PROFILING

Profiling is any form of automated processing of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation,

health, personal preferences, interests, reliability, behaviour, location, or movements. Reasons we might do this include:

- To personalise or improve our products and services.
- To provide you with personalised communications and marketing.
- To create customer or market insights.
- To help us to meet our regulatory obligations (for example, to identify those at risk of becoming financially vulnerable).

14. HOW WE WORK OUT WHAT MARKETING YOU RECEIVE

We use marketing to let you know about products, services, and offers that you may want. This section tells you how we decide what marketing to show or send you. It also explains how we work out what you may be interested in.

We may use your personal information to make decisions about what products, services and offers we think you may be interested in. This is what we mean when we talk about 'marketing.'

When we can use your personal information for marketing

We can only use your personal information to send you marketing messages if we have either your consent or a 'legitimate interest.' That is when we have a business or commercial reason to use your personal information and it does not conflict unfairly with your own interests.

How we decide what marketing may interest you

The personal information we have for you is made up of what you tell us, and data we collect when you use our services, or from outside organisations we work with. We study this to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you. This is called profiling for marketing purposes.

You can contact us at any time and ask us to stop using your personal information this way.

How we send you marketing

We may show or send you marketing material online (on our own and other websites including social media), in our own and other apps, or by email, mobile phone, post or through smart devices and other digital channels.

You can also tell us not to collect data while you are using our websites or mobile apps. If you do, you may still see some marketing, but it may not be tailored to you. See our Cookies Policy for details about how we use this data to improve our websites and mobile apps.

Your marketing choices

You can tell us to stop sending you marketing at any time. Whatever you choose, we'll still send you statements and other important information relating to your existing products and services.

We do not sell the personal information we have about you to outside organisations.

We may ask you to confirm or update your choices, if you take out any new products or services with us in future. We'll also ask you to do this if there are changes in the law, regulation, or the structure of our business.
If you change your mind, you can contact us to update your choices at any time. Please see the 'Your data privacy rights and how to exercise them' section for more information.

15. HOW WE USE YOUR PERSONAL INFORMATION

This section sets out the legal reasons we rely on, for each of the ways we may use your personal information. The law says we must have one or more of these reasons:

- To fulfil a contract we have with you.
- When it is our legal duty.
- When it is in our legitimate interest.
- When you consent to it.
- When it is in the public interest.

When we have a business or commercial reason of our own to use your personal information, this is called a 'legitimate interest'. We will tell you what that is, if we are going to rely on it as the reason for using your personal information. Even then, it must not unfairly go against your interests.

You have the right to object to use of your personal information in this way. You can do this by telling us anything that we may need to consider, to understand if our use of your personal information is fair. Please see the 'Your data protection rights and how to exercise them' section for more information.

The law and other regulations treat some types of information as special, for example, data concerning health. This personal information is called 'special category data'. We will not collect or use these types of personal information without your consent unless the law allows us to do so. If we do, it will only be when it is necessary:

- For reasons of substantial public interest, or
- To establish, exercise or defend legal claims.

Here is a list of all the ways that we may use your personal information, and which of the reasons we rely on to do so. This is also where we tell you what our legitimate interests are where it is the reason for using your personal information. We may rely on different reasons for using the same personal information.

PURPOSE	OUR LAWFUL BASIS	OUR LEGITIMATE INTERESTS (WHERE RELEVANT)
Processing your application for a product or service with us.	• Necessary for the performance of a contract.	N/A.
Identifying customers who require/may require additional support.	• Legitimate interests. • Consent. • Necessary for the performance of a contract.	We may use information about your personal circumstances to support you if you are in, or we consider that you are at risk of being in what is considered to be a 'vulnerable circumstance' (such as experiencing a bereavement or experiencing financial difficulty). This may include placing a `marker' on your account to indicate that you need/might need extra support.
		Before we use special category data (such as information relating to your health), we will seek your explicit consent. However, there may be circumstances where this is not practical/ reasonable, and in these circumstances, we may rely on reasons of substantial public interest to use data where we believe this is necessary to protect your economic wellbeing. For example, this could include situations where without support you: might purchase products or services that could lead to economic harm (e.g., taking out unaffordable credit); could become more exposed to the risk of debt and financial difficulty; might be at risk of financial abuse, fraud, or economic coercion; might not receive communications or advice in a way that allows informed financial decisions to be made; or might be excluded from beneficial processes, products, or services (e.g. product switching, complaints).
To develop and carry out marketing activities.	• Consent. • Legitimate interests.	It is in our legitimate interests to give you information about our products and services that you may be interested in unless we are compelled by legal requirements to obtain your consent.
To study how our customers, use products and services from us and other organisations (e.g., statistical purposes and profiling).	• Legitimate interests.	• Assessing which of our products and services may interest you. • Developing personalised products and services, and what we charge for them. • Defining types of customers for new products or services.

PURPOSE	OUR LAWFUL BASIS	OUR LEGITIMATE INTERESTS (WHERE RELEVANT)
Sending you communications to service your account, products, or services.	• Necessary for the performance of a contract.	N/A.
To develop and manage our brand, products, and services.	• Legitimate interests.	Working out which of our products and services may interest you. Developing products and services, and what we charge for them. Defining types of customers for new products or services.
Carry out data analytics to better understand your circumstances and preferences.	• Legitimate interests.	To help us personalise our products and services to you.
To manage how we work with other companies that provide services to us and our customers.	• Legitimate interests • Necessary for the performance of a contract.	To enable another company to provide you with services you've asked for or check your suitability for products and services.
To develop new ways to meet our customers' needs and to grow our business.	• Legitimate interests.	We do this to improve our products and services to best meet the needs of our member/customers.
Social media.	• Legitimate interests.	We use social media to help connect with you and share information about our products and services. Sometimes these involve using your data. Social media platforms may let you choose what advertising you receive. You should contact them for more information.

PURPOSE	OUR LAWFUL BASIS	OUR LEGITIMATE INTERESTS (WHERE RELEVANT)
Protecting our legal rights.	• Legitimate interests.	We may need to use your information to protect our legal rights (for example, collecting money owed, enforcing, or protecting our security or defending rights of intellectual property); court action; managing complaints or disputes; in the event of a restructuring of companies or other mergers or acquisition. This may be in connection with action taken against you or other persons, for example, joint borrowers or persons who give a guarantee or other security for your obligations to us.
To detect, investigate, report, and prevent fraud and money laundering and verify your identity.	• Legitimate interests. • Legal obligation. • Public interest. • Necessary for the performance of a contract.	• Developing and improving how we deal with financial crime and fraud risks. • Being efficient about how we fulfil our legal and contractual duties. • Protecting our business.
Risk management.	• Legitimate interests.	• To conduct a thorough risk assessment before providing products and services including credit. • To make sure that our business is run prudently (that is, with consideration for what may happen in the future).
To obey laws and regulations that apply to us.	• Legal obligation.	N/A.
To respond to complaints and seek to resolve them.	• Legitimate interests. • Legal obligation.	To make sure that complaints are investigated so that our customers receive a high standard of service, and we can prevent complaints from arising in the future.

PURPOSE	OUR LAWFUL BASIS	OUR LEGITIMATE INTERESTS (WHERE RELEVANT)
To run our business in an efficient and proper way. This includes managing our financial position, business capability, adding and testing systems and processes, managing communications, corporate governance, and audit.	• Legitimate interests.	• To manage risk for us and our members/ customers. • To make sure that our business is run prudently (that is, with consideration for what may happen in the future), and we can recover the debts owed to us, as well as making sure our assets are protected.
Corporate restructuring, merger, acquisition, or takeover, including any transfer or potential transfer of any of our rights or duties under our agreement with you.	• Necessary for the performance of a contract (where personal data must be transferred for contracts to continue to be performed). • Consent. • Legitimate interests.	• To enable us to prepare for the corporate restructuring, merger, acquisition, or takeover. Where practicable, we will aim to wait until all or most of the conditions to closing of the transaction have been satisfied before transferring personal data.
To respond to your request for payment-initiation and account-information services for accounts you have with other providers, or if you have asked a third-party provider to ask us for information, they need so they can provide you with account-information or payment initiation services for accounts you have with us.	• Legal obligation. • Necessary for the performance of a contract.	N/A.
Tracking or recording what you say or do e.g., phone calls, face to face meetings, letters, e-mails, live chats, video chats and any other kind of communication.	• Legitimate interests.	• We may use these to: • Check your instructions to us • Assess, analyse, and improve our service • Train our people. • Manage risk. • Prevent and detect fraud and other crimes.
Capturing CCTV images and recording in our branches and offices for safety and security.	• Legitimate interests	To prevent and investigate fraud, money laundering and other crimes.
Conducting market research and surveys.	• Legitimate interests	We do this to improve our products and services to best meet the needs of our member/customers.
Collecting IP address when using our website.	• Legitimate interests.	• To detect suspicious activities. • To prevent and investigate fraud, money laundering and other crimes. • To protect our business. • To understand where people use our digital services.

16. TRANSFER OF YOUR PERSONAL INFORMATION OUT SIDE THE UNITED KINGDOM (UK)

Your personal information may be transferred to or stored in locations outside of the UK. We will only transfer your data when:

- We're required or permitted to by law or regulatory requirements
- We're sharing data with a third party to support us in the management of your account
- The transfer is compliant with the UK GDPR (General Data Protection Regulations).

When transferring information, we make sure that suitable protection is always maintained by ensuring appropriate safeguards are in place. This could be by:

- Only transferring information to countries that the Information Commissioner's Office (ICO) has deemed to provide an adequate level of protection under Article 45 of the UK GDPR.
- Putting suitable clauses in our contracts so that organisations take appropriate steps to give information equivalent protection as it has in the UK.

You can get a copy of the appropriate safeguards by contacting our Data Protection Officer at: dpo.dpo@thenottingham.com or via our postal address. Please mark the envelope 'Data Protection Officer.'

17. CHANGES TO THIS NOTICE

We keep this Notice under regular review and may change it from time to time. When we make changes, the date at the bottom of this Notice will be updated accordingly. Any modification or amendment to this Notice will be applied as of that revision date. We encourage you to check this from time to time for any updates or changes.

In some cases we may provide additional notice (like adding a banner/statement to our homepage, sending you a notification by e-mail or through signposting in our branches).