



Customer data privacy notice.



What's inside?

1. Our Data Privacy Notice	1
2. Your information	2
3. Why and how we manage your information	3-8
4. Why we use your information	9-13
5. Passing your information to others	14-18
6. Transferring your information outside the UK	19
7. How long we will keep your information	20
8. Your rights	21-23
9. Appropriate Policy Document	24-29

1. Our Data Privacy Notice.

Your information will be held by TSB Bank plc ('TSB').

UK Data Protection Laws require us to manage all personal information in accordance with the Data Protection Principles. In particular, we are required to process your personal information fairly, lawfully and in a transparent manner. This means that you are entitled to know how we intend to use any information you provide. You can then decide whether you want to give it to us in order that we may provide the product or service that you require. All our employees are responsible for maintaining customer confidentiality. We provide training and education to all employees to remind them about their obligations. In addition, our policies and procedures are regularly audited and reviewed.

The TSB apps

We monitor how you use the TSB apps. We also collect information on all the other apps installed on your device, to help us detect malware and potential fraud. This safeguards us all against financial crime.

If we detect suspicious activity or notice that your device is unsafe, we might block your account and your access to the TSB app.

Your information.

We are TSB Bank, 20 Gresham Street, London EC2V 7JA

TSB is committed to providing local banking for Britain. We want you to have trust and confidence in the way we deal with your information.

The UK is a world leader in data protection and privacy. To comply with UK laws, we manage your personal information fairly, lawfully and transparently. This means you'll know how we use your information and we'll tell you about your rights. You can then decide whether you want to give us your information so that we can provide the product or service you need.

Some of the information we receive is known as 'special category data' or 'criminal offence data' and it's considered more sensitive than some other personal data. This is personal data: revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic data; biometric data (where used for identification purposes); data concerning health; data concerning a person's sex life; and data concerning a person's sexual orientation or criminal offence data. When processing this type of information extra care is needed and this is explained in our 'Appropriate Policy Document' which is attached at the end of this Privacy Notice.

All our employees are responsible for maintaining customer confidentiality. We provide training and education to all employees and we regularly review our policies and procedures. Our aim is to make sure that you have confidence in TSB and feel comfortable about giving us your information. We think that safely looking after your information and processing it fairly is a key part of our relationship.

We have a dedicated team that looks after data privacy rights. We also have a Data Protection Officer ('DPO') to guide the business and oversee our use of your information.

The Data Rights Team

TSB Bank
Ariel House
2138 Coventry Road
Sheldon
Birmingham B26 3JW

You can also contact our team by emailing **privacy@tsb.co.uk**

Data Protection Officer

The Data Protection Officer
TSB Bank
Henry Duncan House
120 George Street
Edinburgh EH2 4LH

You can see a copy of this Customer Data Privacy Notice at **tsb.co.uk/privacy**

3. Why and how we manage your information.

Providing our products and services

When you apply for a product or service, and throughout our relationship, you'll provide personal information to us.

We'll also collect certain information about you from others, including people who may be acting on your behalf. We will gather and process the type and amount of personal information that is relevant and required, and use this personal information to do all of the things you expect from us. And to meet our obligations to you under our Terms and Conditions, this includes:

- checking your identity and confirming that it is you
- managing your relationship with us
- providing you with products and services
- checking your credit reference and that you can afford products and services
- recording money in and out of your accounts
- telling you about important changes or developments to the features and operation of these products and services
- updating, consolidating and improving the accuracy of our records

- crime detection, prevention and prosecution
- carrying out financial reviews
- responding to your enquiries and complaints
- administering offers, competitions and promotions
- arrears and debt recovery activities
- reporting to regulators
- testing systems and processes

We won't be able to open or maintain a product or service if you fail to provide certain information.

Occasionally TSB receives names and addresses (including email addresses) of noncustomers who it's thought may be interested in our products and services.

In these circumstances, where we have your consent, we'll let you know by email or post of the products or services we believe maybe of interest. If we don't already have your consent, we'll tell you about our products and services by post in accordance with our legitimate interests to promote our business. You have the right to opt out of this marketing at any time, by following a link on the email or by contacting our Data Rights Team.

3. Why and how we manage your information



Whose data will we receive?	What type of data will we receive?	Who will send us data?
All TSB customers.	Data confirming your identity. Data relating to credit history and status of you or any associated person. Data relating to any fraudulent activity or suspected fraudulent activity concerning you or any associated person. Data relating to Politically Exposed Persons (PEPs).	Credit Reference and Fraud Agencies. See more information below. CIFAS, a not-for-profit fraud prevention membership organisation. For more information on CIFAS go to www.cifas.org or write to: Consumer Affairs, CIFAS 6th Floor Lynton House 7-12 Tavistock Square London WC1H 9LT
Joint account holders.	Where one person opens a joint account they'll provide us with the name and address of the joint account holder, who will also become a TSB customer.	The person who opens the account, or adds the joint account holder to an existing account.

3. Why and how we manage your information

Whose data will we receive?	What type of data will we receive?	Who will send us data?
TSB Added Value Accounts (TSB AVA). If you hold a TSB AVA, we work with business partners to provide the additional benefits to you.	These business partners will pass your personal data to us if it is relevant to our relationship with you. For example, they'll inform us if you notify them of a change in your contact details. They'll also tell us if you make a claim on an insurance product provided under the TSB AVA. However they will not normally provide us with details of the claim.	TSB's business partners, where you choose to use their products or services in association with TSB.
Guarantors, deposit providers, and similar.	If a person guarantees to pay TSB any sums that a TSB customer may owe, or provides a deposit (for example when a TSB customer takes out a mortgage) we'll record enough details to let us contact them if/when needed. Where they provide the deposit from their bank account, we'll record the account details.	The TSB customer.



3. Why and how we manage your information

Whose data will we receive?	What type of data will we receive?	Who will send us data?
Property vendors, employers and others who interact with TSB customers.	If a person takes out a TSB mortgage to purchase a property they will, in most cases, give TSB the vendor's name and address. Where another person pays the mortgage deposit, TSB will note the name, address and account details of the person paying the deposit. In some circumstances, TSB customers provide us with their employer's details, such as name, address and payroll number.	The TSB mortgage holder.
Providers of professional services.	Business/trading name, address, contact details, internal reference, membership of professional bodies, levels of insurance (if any), identity of client and other information provided to us in the course of delivering the professional services in question	TSB customer; the person or organisation you are providing professional services to, professional bodies and public sources.
Mortgage customers.	Name, address, property details, financial details.	Your mortgage advisor.



Providing products with other service providers

As well as our core banking services, TSB combines with others to provide additional services. We do this where we believe it's in your interests and ours, or where it's necessary to deliver the service you've asked for. This involves passing some of your personal information to TSB business partners who help provide these products. We only pass the minimum information needed to these TSB business partners. And we always make sure that your information remains protected as required under UK law, including laws regulating the sending of marketing messages to you.

Where you apply for a product or service that's delivered with a business partner, we'll collect your personal information and use it to process your application and provide these services in the ways described as follows:

TSB's Added Value Accounts (TSB AVAs)

TSB's Added Value Accounts give customers a range of products and benefits, depending on the accounts you hold and the products and benefits you choose. These products are provided by our business partners. They'll be made known to you when you select the relevant product.

3. Why and how we manage your information

To help you benefit from these products, TSB must pass the information you give us to the business partner providing the service. For example, if you take out mobile phone insurance, details of your handset may be passed to the business partner providing the insurance.

These business partners are separate data controllers. They'll tell you about any information they hold that relates to you, what they do with it and why. They'll also give you their contact details and tell you about your privacy rights.

TSB will work with these business partners to give you the best possible service. This involves some information continuing to pass between them and TSB. They'll let us know when you make use of the product or service. If you tell either TSB or the business partner that your contact details have changed, they'll let each other know to keep records up-to-date.

It's a good idea to make sure you give both TSB and the relevant partner your up-to-date contact details. They'll also pass to TSB high level information about the take-up of the products by TSB customers and benefits provided or claimed. But they won't provide details of individual customers. Where there is a dispute, they'll pass information to TSB to help us deal with the dispute.

Why we use your information.

We use your information so we can deliver the banking service that Britain wants in the 21st century. This includes using your information so we can:

Determine your eligibility

Like all banks, when you apply for products or services, we use automated processes to carry out financial reviews and make faster decisions (for example determining your eligibility for an account or loan). But we want to make sure this works for you and us.

We'll use automated processes to help decide whether you're eligible for a particular product, the appropriate amount of credit that we should provide, and to carry out credit and fraud prevention checks. Due to the sheer amount of information involved and the volume of applications, routine human involvement is impractical or impossible. So to allow us to provide banking services, we need to do this work in an automated way. Some fraud checks that we carry out are necessary to meet our legal obligations.

Based on the information you provide us, we'll compare this against different metrics to determine whether you meet the eligibility criteria for an account. Or to determine whether you'll be able to make repayments on a product.

We work hard to make sure we make the right decision. Sometimes this means saying no to offering you an account or product. In making these decisions, we'll pass information to, and receive information from, Credit Reference Agencies.

If we make an automated decision on something important to you, we'll always allow you to contest the decision, give your views and make sure there's proper human involvement. If you want to exercise this right, please contact our Data Rights Team using the details shown on **page 2**. Where possible you should provide any additional relevant information you'd like us to consider. The logic and outcomes of this decision-making are tested regularly to make sure they're fair.

Improve our performance

We'll use your information to make sure we give you and other customers the best possible service.

This includes testing new systems, checking processes, checking upgrades to existing systems, training, undertaking transactional analysis, conducting audits and assessing lending and insurance risks. It also involves customer modelling, statistical and trend analysis aimed at developing and improving products and services, as well as providing information to Regulators. We do this to meet our legitimate interests in providing better services to our customers and making sure your information is appropriately protected.

To undertake consumer experience research, we may pass your contact details to our trusted third party market research companies, who may contact you on our behalf to conduct surveys and provide us with the results of your customer experience. We will use this information to develop products, services and process improvements. You will be given the opportunity to opt-out of these.

Improve security and combat fraud

We use biometric data analysis to combat fraudsters. When you use a debit or credit card to purchase goods or services online we will ask you to enter your email address, as well as a one-time password sent to your phone at the point of payment.

Although we won't store or check your email we will use biometric data analysis to assess the unique way you type your email and the one-time password as part of our identity verification. So should anyone else try to use your credit card or debit card to make an online purchase, we'll be alerted to it because of the way they enter your details. We also analyse how you use the App to keep your accounts safe. The lawful basis for this is the substantial public interest of combatting fraud.

Send direct marketing and promotional material

We take great care to make sure that information you receive from TSB Bank is likely to be of interest to you. We do this by comparing our range of products and services with what we know about your needs and interests. We may 'profile' TSB customers to allow us to identify relevant opportunities to promote TSB services to individual customers or prospective customers. This may include reviewing historic and current data about which account or services you hold, the way you operate your accounts, your account balances and the transactions on your TSB accounts. This could include analysis of individual payments in and out of your accounts.

The profiling we carry out will aim to ensure the marketing of our products and services is likely to be of interest to you. We'll do this through TSB channels, such as our branches, websites, mobile apps, telephone service; or through non-TSB channels, such as social media, websites, radio or TV advertising.

The lawful basis for the profiling we do, and any tailored marketing through these channels, is our legitimate interests. This means we have a legitimate interest in carrying out these activities in order to promote our business and to help ensure that our customers only receive useful information which is likely to be of interest to them. You can object to this by contacting our Data Rights Team. This means you'll see more general marketing, and the pages and ads may be less relevant to you; the number of advertisements will generally remain the same.

We value our relationship, so we do our best to only send you information we think may be of interest to you personally. You decide if you want to receive direct marketing from us, whether by post, email, phone or text message.

We'll only send direct marketing to TSB customers in this way if you've consented to receive it. And don't worry, you can withdraw your consent at any time. Simply contact our Data Rights Team, click 'unsubscribe' in any marketing email we send you, or follow the instructions in our marketing text messages.

Make the most of social media

If you interact with TSB through social media we may use your information to help us communicate.

To deliver the best customer experience, we partner with software providers that allow us to connect with you via online communities and blogs. These partners manage personal information only in accordance with our instructions. TSB can also require these partners to delete your information, or return it securely to TSB, at the end of our contract with them.

Do what you ask us to do

If you request particular services from us, or ask a question, we'll use your personal information to respond. This is to make sure we can provide the best possible service.

Comply with legal obligations

This might include providing information to HMRC, preventing fraud and money laundering and doing what our Regulators require. We only do this where strictly necessary to comply with these legal obligations.

Delivering better banking

This includes using personal information to make sure we:

- manage and develop customer relations
- assess the suitability of existing and proposed products for our customers
- pass information to Credit Reference Agencies (as described below)
- conduct internal or external reviews of our performance and quality
- instruct our internal or external legal teams
- detect and prevent fraud and liaise with police and other anti-fraud agencies
- engage with and interact on social media
- make sure we manage TSB as effectively and efficiently as possible.

We use your personal information in this way as it's in our business interests. It also allows us to defend our rights, provide a better service to our customers and understand what our customers want from us. Whenever we use your personal information, we'll always make sure we work to protect your interests and rights. We won't use your personal information for any purpose incompatible with those set out above.

We'll keep your data appropriately secure, and let you know if we use it for a new purpose.

Occasionally we'll ask for your specific consent to use your personal information. This might be when we want to record sensitive information, such as details about your health or ethnicity.

Asking for your consent gives you control over how this information is used. You can withdraw this consent at any time.



5. Passing your information to others.

We treat your personal information as private and confidential. In some instances we may disclose it outside TSB for the purposes set out above (including sharing information with partners who help us provide services). This may include sharing it with subcontractors. They'll act solely on our instructions or behalf and will only use your information for the purposes set out above.

We'll disclose information to others to meet our contractual obligations to you in accordance with the Terms and Conditions, including where:

- your information relates to a joint account, where the other account holder(s) may be entitled to see your transactions
- it's needed by other parties connected with your account (including guarantors)
- we need to share information with other lenders who also hold a charge on your property.

We'll also disclose information where strictly necessary to comply with our legal obligations, including where:

- HMRC or other authorities require it
- the law, a regulatory body or the public interest requires it
- it's required as part of our duty to protect your accounts. For example we are required to disclose your information to the UK Financial Services Compensation Service (FSCS)
- it's required by us or others to detect, investigate or prevent crime or fraud.

Information can also be made available where you consent or ask us to. If you give your consent, you can withdraw it at any time and we'll stop disclosing the information in that way.

Credit Reference Agencies

In order to process your application for a product or service, we'll perform credit and identity checks on you with one or more credit reference agencies ('CRAs'). If you use our banking services we may also make periodic searches at CRAs to help manage your account.

To do this, we'll supply your personal information to CRAs and they'll give us information about you. This will include information from your credit application and about your financial situation and history. CRAs will supply us with public data (including the electoral register) as well as shared credit, financial situation, financial history and fraud prevention information. We'll use this information to:

- assess your creditworthiness and whether you can afford to take out a product
- verify the accuracy of the data you've provided
- prevent criminal activity, fraud and money laundering
- manage your account(s)
- trace and recover debts
- make sure any offers provided to you are appropriate to your circumstances.

We'll continue to exchange information about you with CRAs while you have a relationship with us. We'll also inform them about your settled accounts. 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 from us they'll place a search footprint 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. So make sure you discuss and share this information with them before sending the application. CRAs will also link your records together. These links will remain on both your files until such time as you or your partner successfully files for a disassociation with the CRAs to break that link.

The identities of CRAs, their role 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 CRAs are explained in detail at **www.experian.co.uk/crain**. CRAIN is also accessible from each of the CRAs that TSB uses – visiting any of these links will take you to the same CRAIN document:

TransUnion **www.transunion.co.uk/crain**
Equifax **www.equifax.co.uk/crain**
Experian **www.experian.co.uk/crain**

Fraud Prevention Agencies

To make sure we help in the international fight against terrorism, money laundering, modern slavery and other criminal activities, the government requires us to screen applications made to us. As a result, we will disclose information to fraud prevention agencies and to government bodies. If we think there is a risk of fraud, we may block access or stop activity on an account.

We will study patterns of activity, check for unusual transactions and monitor devices used to access TSB's systems, including Internet Protocol (IP) addresses and this may include using widely available geographical mobile phone or other technology to assess the location where you or any devices may be located.

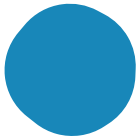


Data-sharing with our parent company

TSB Bank plc is owned by Banco de Sabadell. In order for Banco de Sabadell and/or TSB to comply with legal obligation(s) to report to European capital risk supervisory regulators and/or UK regulators or because it is in our legitimate interests to do so, we will share personal data with Banco de Sabadell in their capacity as a data controller or processor, for that purpose. The data shared will be within the EEA* and is therefore protected to a similar standard to when it is in the UK.

You have the same rights with regards to Banco de Sabadell's processing as you do when TSB is processing/using your personal data and these rights are explained in section 8 below. Should you wish to exercise rights in relation to our parent company's processing, please contact Banco de Sabadell's dedicated data rights team at: Derechos PD, a través de su domicilio, Alicante (03007), Avda. Óscar Esplá nº 37, 03007, Alicante, Spain or by email: ejercicioderechosprotecdatos@bancsabadell.com.

The personal data shared will generally be held for up to six years depending on the reporting required. For example, where the data is used to identify if customers have more than one holding across the Group to meet regulatory requirements or enable reporting to the EU and UK regulators, non-matched data will be



retained by Banco de Sabadell for three months and matched data for six years.

If you have a problem with accessing your information or you are concerned about the way Banco de Sabadell has handled your information then, in addition to complaining to the ICO, you can also complain to the Spanish data protection regulator: Agencia Española de Protección de Datos (“AEPD”): www.aepd.es.

Further information about Banco de Sabadell’s processing can be found in their general customer information notice: www.bancsabadell.com and their Data Privacy Notice which is available [here: DPN](#)

* Countries that belong to the EEA: Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

General

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.

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.

Details of the personal information that will be processed include, for example: name, address, date of birth, contact details, financial information, employment details, device identifiers including IP address and vehicle details.

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

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.

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.

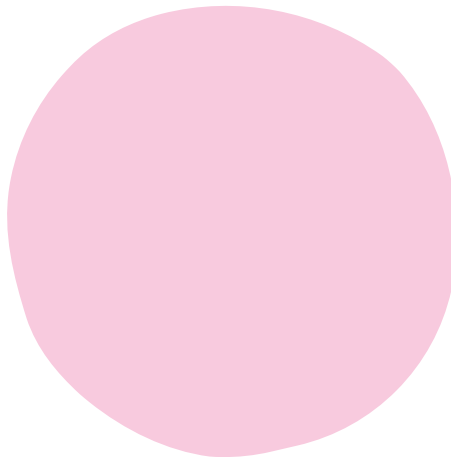
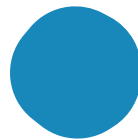
Consequences of processing

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.

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 using the details on **page 2**.

Data transfers

Whenever fraud prevention agencies transfer your personal data outside of the European Economic Area, they impose contractual obligations on the recipients of that data to protect your personal data to the standard required in the European Economic Area. They may also require the recipient to subscribe to 'international frameworks' intended to enable secure data sharing.



6.

Transferring your information outside the UK.

The UK and other EEA countries* provide a high standard of data protection and privacy. However we may run your accounts and provide other services from centres outside the UK and EEA that do not have a similar standard of data protection laws. If so, we'll require your personal information to be protected to at least UK standards.

So we only transfer personal information to:

- countries that have been confirmed as protecting personal information to UK and EU standards.
- companies in the USA certified as providing an adequate level of protection.

In other instances, we'll put contractual commitments in place which make sure personal information is protected to UK and EU standards.

If you want to learn more about the specific countries to which we transfer personal data, or need a copy of the safeguards we have in place for particular countries, contact the Data Rights Team.

We may process payments through other financial institutions, such as banks and the worldwide payments system operated by the SWIFT organisation. For instance, this can happen if you make a CHAPS or foreign payment. These external organisations may process and store your personal information abroad and may have to disclose it to foreign authorities to help them in their fight against crime and terrorism. If these are based outside the UK and EEA, your personal information may not be protected to standards similar to those in the UK. However we'll take steps, including using contractual commitments, to make sure that an adequate level of protection is provided.

* Countries that belong to the EEA: Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden.

7.

How long we will keep your information.

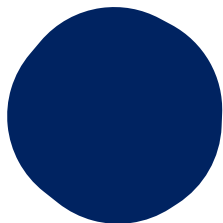
We'll keep your information for as long as your account or product application takes. And for as long as you have accounts or products with us. We'll also keep your personal information for a certain period after your application has ended or you've closed your accounts.

When determining how long this period will last, we take into account our legal obligations, the expectations of financial and data protection regulators, and the amount of time we may need to hold your personal information to carry on our business or defend our rights. For example, if you have an account with TSB, we'll keep your information and account details

while the account is open. To meet our legal and regulatory requirements, we must keep much of this information for a number of years after the account is closed – even if you do not have another account with us.

We'll also need to keep your information in archived form in order to defend our legal rights. This may be for the period during which legal claims can be made under applicable law. In the UK this is six years for contractual claims. We have policies and procedures in place to make sure that we delete information no longer needed for any of these purposes.

If we are not able to completely delete, destroy or anonymise your personal information within these times because, for example, there are inter-dependencies between IT systems, we will limit access to your personal information or put it beyond use wherever possible.



You have certain rights over your personal information. These include the right to access a copy of your personal information, or have some elements of it transmitted to you or another company in a common electronic format. In certain circumstances you can have your personal information corrected or erased, or you can restrict our use of it. You also have the right to object to the way we use your personal information as described above.

We generally won't charge you to exercise these rights. You have the following rights:

Access

You have a right to ask TSB if we have your personal information. If we do, you have a right to know:

- why we have it
- what type of information we possess
- whether we have or will send it to others, especially outside the European Economic Area (for a list of EEA countries, see **page 19**)
- how long we will keep it
- where we got it from
- details of any automated decision-making.

If you want, you can ask for a copy of your information.

Rectification

Where any of your information is incorrect, you have a right to tell us to correct it promptly. Please tell us as quickly as possible if you change your address or other contact details. If your information is incomplete, you can ask us to correct this too.

In certain circumstances, you have the following rights:

Object

Depending on the legal basis for which we are using your information, you may be entitled to object. For example, where we're using your information connected with marketing, we will stop if you object. However, if we're using your information to meet certain legal obligations, we may continue to do so even if you object.

Erasure

You may have a right to have some or all of the information we hold about you deleted. However you should be aware that, as a bank, we are required to retain many records even after you close your account. Please see the 'How long we will keep your information' section above for further information.

Portability

In certain circumstances you are entitled to receive some of your information from us electronically. We can either pass the information to you, or to another person or business if you want.

Restriction

You might also be entitled to ask us to restrict our use of your information – for example if you think the information we hold on you is incorrect.

Automated decision-making

We'll use automated systems to make decisions about whether you're eligible for a particular account or products, and to carry out credit and fraud prevention checks. Based on the information you give us, we'll compare this against different metrics to determine whether you meet the eligibility criteria for an account, or to work out whether you'll be able to make repayments on a product.

We work hard to make the right decision. Sometimes this means saying no to offering you an account or product. If we make an automated decision on something important to you, we'll always allow you to contest the decision, give your views and make sure there's proper human involvement. The logic and outcomes of this decision-making are tested regularly to make sure they're fair.

Consent

If you consent to us using your information, you have the right to withdraw that consent at any time.

You can exercise these rights by contacting the Data Rights Team using the details shown on **page 2**.

We aim to work with you on any request, complaint or question you have about your personal information. However, if you believe we have not adequately resolved a matter, you have the right to complain to the Information Commissioner's Officer (the 'ICO').

In the event that we identify instances of non-compliance by the Bank we will notify the ICO directly where required.

You have a right to complain to the ICO. As an independent UK authority, it upholds information rights in the public interest, promotes openness by public bodies and data privacy for individuals. You can visit their website at <https://ico.org.uk> for further information or ask for details from our Data Rights Team.

Appropriate Policy Document.

Our Appropriate Policy Document explaining our use of special category and criminal offences data is available [here](#).

Appendix

Special Category Data

Appropriate Policy Document

Processing of special categories of personal data and criminal offence data.

As part of TSB's functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

Special category data

Special category data is defined at Article 9 GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health; or
- Data concerning a natural person's sex life or sexual orientation.

Criminal offence data

Article 10 GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'. For the avoidance of doubt criminal offence data is not in itself special category data.

This policy document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement.

The information supplements our privacy notice and staff privacy notice.

Conditions for processing special category and criminal offence data.

We process special categories of personal data under the following GDPR Articles:

i. Article 9(2)(a) – explicit consent

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include staff dietary requirements and health information we receive from our customers who require a reasonable adjustment to access our services.

ii. Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on TSB or the data subject in connection with employment, social security or social protection.

Examples of our processing include staff sickness absences and checking if individuals are entitled to work in the UK.

iii. Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

Examples of our processing include where an individual needs emergency medical services but is unconscious or otherwise incapable of giving consent.

iv. Article 9(2)(f) – if processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

Examples of our processing include processing relating to litigation in relation to collection and recoveries.

Article 9(2)(g) – for reasons of substantial public interest.

Examples of our processing include the information we seek or receive as part of investigating fraud.

We process criminal offence data under Article 10 of the GDPR.

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.



Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an Appropriate Policy Document (see Schedule 1 paragraphs 1 and 5).

This section of the policy is the Appropriate Policy Document for TSB. It demonstrates that the processing of special category and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the GDPR Article 5 principles. In particular, it outlines our retention policies with respect to this data.

Description of data processed

We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any trade union. Further information about this processing can be found in our staff privacy notice.

Our processing for reasons of substantial public interest relates to the public good, or what is in the best interests of society. This includes ensuring equality or preventing fraud. Further information about this processing can be found in our privacy notice.

We also maintain a record of our processing activities in accordance with Article 30 of the GDPR.

Schedule 1 conditions for processing

We process Special Category Data for the following purposes in Part 1 of Schedule 1:

Paragraph 1(1) employment, social security and social protection.

We process special category data for the following purposes in Part 2 of Schedule 1. All processing is for the first listed purpose and might also be for others dependent on the context:

- Paragraph 8(1) equality of opportunity or treatment
- Paragraph 9(1) racial and ethnic diversity at senior levels
- Paragraph 10(1) preventing or detecting unlawful acts
- Paragraph 11(1) and (2) protecting the public against dishonesty
- Paragraph 12(1) and (2) regulatory requirements relating to unlawful acts and dishonesty
- Paragraph 14(1) and (2) preventing Fraud
- Paragraph 15(a) and (b) suspicion of terrorist financing or money laundering
- Paragraphs 18(1) to (4) safeguarding children and individuals at risk
- Paragraph 19(1), (2) and (3) safeguarding of economic well-being of certain individuals
- Paragraphs 20(1) to (7) insurance
- Paragraphs 21(1) to (4) occupational pensions

- Paragraph 24(1) and (2) disclosure to elected representatives

Criminal offence data

We process criminal offence data for the following purposes in parts 1 and 2 of Schedule 1:

Paragraph 1 – employment, social security and social protection

Procedures for ensuring compliance with the principles

Accountability principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a Data Protection Officer who reports directly to our highest management level;
- Taking a 'data protection by design and default' approach to our activities;
- Maintaining documentation of our processing activities;
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors;
- Implementing appropriate security measures in relation to the personal data we process;
- Carrying out data protection impact assessments for our high risk processing.

We regularly review our accountability measures and update or amend them when required.

Principle (a): lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

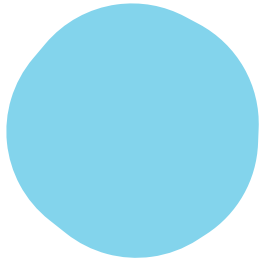
We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice, staff privacy notice and this policy document.

Our processing for reasons of substantial public interest relates to the public good, or what is in the best interests of society. This includes ensuring equality or preventing fraud. Further information about this processing can be found in our privacy notice.

Our processing for the purposes of employment relates to our obligations as an employer.

Principle (b): purpose limitation

We process personal data for purposes of substantial public interest as explained above where it is necessary for complying with or assisting another to comply with a regulatory requirement to establish whether an unlawful or improper conduct has occurred, to protect the public from dishonesty, preventing or detecting unlawful acts or for disclosure to elected representatives.



We may process personal data collected for any one of these purposes (whether by us or another controller), for any of the other purposes here, providing the processing is necessary and proportionate to that purpose.

If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

We will not process personal data for purposes incompatible with the original purpose it was collected for.

Principle (c): data minimisation

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Principle (d): accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Principle (e): storage limitation

All special category data processed by us for the purpose of employment or substantial public interest is, unless retained longer for archiving purposes, retained for the periods set out in our retention schedule. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs. Our retention schedule is reviewed regularly and updated when necessary.

Principle (f): integrity and confidentiality (security)

Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures.

Our electronic systems and physical storage have appropriate access controls applied.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

Retention and erasure policies

Our retention and erasure practices are set out in our retention schedule.

Appropriate Policy Document review date

This policy will be retained for the duration of our processing and for a minimum of 6 months after processing ceases.

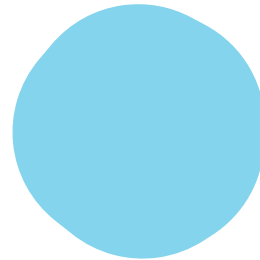
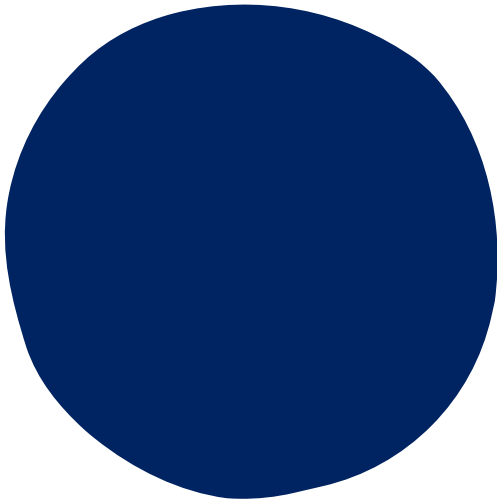
This policy will be reviewed annually or revised more frequently if necessary.

Additional special category processing

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document.

Our processing of such data respects the rights and interests of the data subjects.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and staff privacy notice.





Need some extra help to do your banking? This might be due to physical or mental wellbeing or a life event. We're here to support you. Let us know what you need by calling **03459 758 758**, chat to us in the Mobile Banking App, or visit us in branch.

This information is available in large print, braille and audio. Ask in branch or call us on **03459 758 758** (lines are open from 8am to 8pm, 7 days a week).

If you have a hearing or speech impairment you can call us using the Relay UK service. Type '18001' before entering our telephone number. A member of the Royal National Institute for Deaf People will join the call to speak with us as you send and receive text messages. Please visit **www.relayuk.bt.com** to read how they manage your data.

If you need to call us from abroad, or prefer not to use our **0345** number, you can also call us on **+44 203 284 1575**. Calls may be monitored or recorded.

TSB Bank plc. Registered Office: Henry Duncan House, 120 George Street, Edinburgh EH2 4LH. Registered in Scotland No. SC95237.

Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Registration No. 191240). TSB Bank plc is covered by the Financial Services Compensation Scheme and the Financial Ombudsman Service.

