

About the terms of use

Thank you for registering for digital banking. Our digital banking services offer you several ways to do your banking on-the-move through our digital channels.

1 When the terms of use apply

The terms of use are a legal agreement between you (the individual or legal entity using digital banking) and us and they apply as follows:

- 1.1 when you register for digital banking; and
- 1.2 whenever you use digital banking.

2 Promises that you make to us

You warrant that:

- 2.1 you can enter into a contract (you have full contractual capacity) and no court has declared you mentally unfit to do so;
- 2.2 you gave us accurate information when you registered for digital banking; and
- 2.3 you read and understood the terms of use before you accessed digital banking.
(To warrant something is to promise that it is true, and we have the right to rely on the truth of your statement.)

3 Additional terms and conditions also apply

- 3.1 The terms of use, including any definitions, privacy statements and disclaimers that are incorporated by reference into the terms of use, apply together with the latest version of the General terms and conditions and the product terms applicable to your account, all of which are accessible through our digital channels.
- 3.2 If there is any conflict between the terms of use and the other terms mentioned in this clause, the terms of use will apply to your use of digital banking.

4 We may change the terms of use

- 4.1 We may change the terms of use at any time. We'll announce changes or updates to the terms of use through our digital channels or our website, by email or SMS or on WhatsApp.
- 4.2 The most recent version of the terms of use applies to you each time you access digital banking. By continuing to use digital banking you agree to the most recent version of the terms of use.

5 Contact us if you have any questions

We want our interactions with you to be fair and transparent, so we've designed the terms of use to be simple and clear. If there is anything you would like to ask us, you can contact us as follows:

- 5.1 By phone on **0860 123 000**; or
- 5.2 By email at **information@standardbank.co.za**; or
- 5.3 Through our complaints process, which you can find on our website by clicking on the "Contact Us" tab.

6 Definitions

The words below have the meanings set out next to them unless the context clearly indicates a different meaning.

access codes	means the unique combination of numbers, letters, symbols and other data that you use to access digital banking, such as username, passwords, personal identification numbers (PINs), card numbers, one-time passwords (OTPs), email addresses or biometric information (including facial and fingerprint recognition).
account	means any credit facility, transactional, savings or investment account that we open in your name at your request, and that can be accessed through the digital channels.
cellphone banking	means digital banking via USSD through a cellphone.
device	means the equipment that you use to access digital banking, such as your cellphone, computer, tablet, smart TV, ATM or other equipment.
digital banking	means doing your banking through our digital channels using a device.
digital channels	means the digital ways in which we provide banking to you, including cellphone banking, Internet banking and the mobile banking

app, as well as any other channels we may add.

Instant Money

means a service that allows you to send money to someone else through our digital channels and other means

**Internet banking
mobile banking app**

means digital banking through the Internet
means digital banking through the Standard Bank/Stanbic Bank mobile banking application.

prepaid purchases

are transactions where you pay in advance for selected products and services such as electricity, airtime and data bundles.

profile

means the digital profile of an individual or legal entity that we create for you when you register for digital banking.

Standard Bank, we, us, our

means The Standard Bank of South Africa Limited (Registration Number 1962/000738/06) and its successors or assigns.

transaction

means any debit or credit on your account that we process according to your instructions.

7 Using digital banking
7.1 The Standard Bank mobile banking app is free but there may be data costs

Standard Bank does not charge you to download or use the mobile banking app or cellphone banking. Your mobile network or Internet service provider may charge you data costs for this.

7.2 Create secure login details and protect it

When you use digital banking, there's no direct personal contact between you and us. You communicate with us using a device. When you register for digital banking, you must create secure login details using access codes. You'll need to enter these access codes each time that you use digital banking.

7.3 Your access codes are the same for all devices

You can download the mobile banking app onto more than one device but only one mobile banking app on any one device. You don't need to re-register for digital banking on each device, but you must use the same access codes.

8 Keeping safe on digital banking
8.1 Your access codes

- a) Keep your access codes secret and safe
 - You must keep your access codes secret and safe and protect your device. If someone else discovers your access codes, they could:
 - i. access your profile and your accounts either through the same device or through a different digital channel;
 - ii. perform transactions on your accounts;
 - iii. steal money from your accounts;
 - iv. use your account information illegally;
 - v. apply for a credit facility, for example an overdraft or a loan;
 - vi. apply for an overdraft limit increase or change your credit limits;
 - vii. make an international payment, which could affect your single discretionary allowance;
 - viii. change your ATM or EAP limits.
- It's not safe to keep your access codes on your device.
- b) Don't share your access codes with anyone else
 - i. You must never allow any person, including our employees, or any software to discover your access codes. No-one has a reason to know or ask for your access codes. If someone has asked you for any of your access codes or you think they may know the codes, you must contact our client contact centre or your branch immediately.
 - ii. You accept that you alone are responsible for:
 - keeping your access codes secret and safe;
 - preventing other people or software from discovering your access codes; and
 - any activity that takes place on your profile if you have shared or compromised your access codes.

iii. You agree that we may receive instructions that appear to be from you but that you did not authorize, and we will act on all instructions that appear to come from you, if you don't keep your access codes secret and safe: iv. you agree that we're not responsible for any loss that you may suffer; and v. you give up any rights you might have to claim against us for any loss that you may suffer. c) If we are asked to change or deactivate your access codes We take your security seriously. If we receive a request that appears to come from you to deactivate or change your access codes, we'll take one or more of the following steps, where appropriate: i. ask you to prove your identity to us; ii. reject any banking instructions we receive; iii. stop a transaction if possible (this happens if we have not already carried out your banking instruction); iv. reverse payments if possible from the time we think someone started using your access codes without permission; or v. deactivate your access codes (but we won't always be able to tell you before we do this).	9 9.1 9.2 9.3 9.4 9.5	About transacting on digital banking Check that you enter the correct details for transactions You must make sure you enter the correct details for your transactions. We are not responsible for any loss that you suffer if you enter the wrong details for your transaction. Transactions cannot be stopped after you send them You cannot cancel, change or stop a transaction after you have sent it to us. You cannot reverse a transaction, even if it's a transaction you have repeated by mistake. We are not responsible for any loss that you may suffer as a result. Check that we've received your instruction You mustn't assume that we've received your instruction for a transaction. We'll usually inform you on your device that we've received your instruction. If you're not sure that an instruction has gone through, you can contact our Client Contact Centre or check your bank statement. Don't give the same instruction again unless we've told you that we did not receive it as a payment might go through twice. Transactions might not show immediately If you send an instruction after 7pm (South African time), your statement will show that the transaction went through on the next business day.
8.2 Check the Security Centre for guidelines regularly We've set up a Security Centre on our website with guidelines on how to protect yourself against theft and fraud when using digital banking. These guidelines change regularly as we keep updated with new scams. It's your responsibility to check our guidelines regularly and to comply with our advice.		Managing limits on transactions a) Limits on payments We set a default payment limit for your electronic payments on digital banking to protect you from unauthorised payments. This is called the Electronic Account Payment (EAP) limit, and it can be changed on your profile. It's your responsibility to manage your EAP limit.
8.3 We check information that you send to us To limit the risk of fraud or theft on your account, we may check any information you send to us through digital banking.		b) Limits on prepaid purchases and Instant Money transactions There may be limits on some prepaid purchases and Instant Money transactions. You can change these limits at a branch or by using an ATM. You cannot change them on your profile.
8.4 Don't use public devices for digital banking Don't use any public device, for example a computer at an Internet café, to access digital banking. Public devices are not safe because you don't know what software or hardware may be on them. For example, they may use spying technology to find out numbers or passwords you type on a keyboard. These could be used to get into your account to defraud you or steal money.		9.6 Make sure your account has enough money for payments and fees a) You must make sure that there is enough money in your account for: i. payments, including scheduled and repeat payments; and ii. the fees related to the payment. (We might not process payments if you don't have enough money in your account. If you transfer money into your account, you must make sure it reaches your account at least 24 hours before the payment is due to be made.)
8.5 De-link devices that you no longer have or that are lost or stolen If any device on which you have digital banking is lost or stolen or not in your possession, you must immediately log in to your digital banking profile on another device and de-link your device or your profile or both. We are not responsible for any losses that you may suffer because you didn't de-link that device or your profile. If you cannot immediately de-link, call our Fraud Helpline at 0800 222 050 for assistance.		b) Some transactions that may take your account balance below zero might go through. If this happens, you remain responsible for the transactions and you must transfer money into your account to bring it back to at least zero. We may debit any other account that you hold with us to cover fees for those transactions.
8.6 Don't give information in response to emails, SMSes and phone calls asking for your information We'll never ask you by email or SMS or through other digital messaging to access a link. You must not respond to requests to transfer money or to enter or confirm your access codes through any of the following channels: a) emails – such a request is known as phishing b) SMSes – this type of request is known as smishing c) telephone calls – this is known as vishing d) any other digital message.	10 10.1	Information we provide through digital banking General information only a) We don't offer to do business with you i. We give general information on our digital banking platforms. For example, we may give information about: • our plans, goals and estimates for our future operations and services; • returns on investments, estimated income from investments, capital expenses, shares or other financial items; and • our estimates of the economy's future performance. ii. We give the information to make you aware of the products and services that we offer, as well as how some of our products might perform. We don't give the information as an offer of a product or service for you to buy, sell or deal in any investments unless we clearly state that it is an offer. We don't ask you to enter into any agreements with us through digital banking unless we clearly state it.
8.7 Keep your device safe from SIM card swaps If a fraudster accesses your SIM card information from your device, they can intercept messages between you and us. Keep your device safe at all times. If you lose your device or if it is stolen, contact your cellphone or data provider immediately to block the SIM card.		b) Information might be old Refresh your screen regularly to make sure that the information you see is the latest that is available through our digital channels. News or market information, such as share prices or data, is updated regularly but may be at least 30 minutes old.
8.8 Properly end your digital banking sessions every time After every digital banking session, you must properly end your session by logging out of your profile and closing the digital channel. If you don't properly end your digital banking session, someone you haven't authorised might be able to access your account and your money. They may commit fraud on your account or steal your money. We are not responsible for any losses that you suffer if this happens.		c) We cannot promise that the information is correct We may add information that we gather from other organisations on digital banking. This information is not given by or for us. We have no control over it and don't confirm or guarantee that it is correct or suitable for you.
8.9 Report suspicious activity immediately You must report suspicious activity immediately. You can contact: a) our Fraud Helpline at 0800 222 050 (+27 10 249 0700 for international callers); or b) our Client Contact Centre at 0860 123 000.		

- 10.2 **Links to content belonging to others**
- d) We may provide links to content created by other people or entities. We aim to link you only to trustworthy sources, but we cannot guarantee the accuracy or reliability of the information they provide.
 - e) If we give a link to any other information, person or entity, this does not mean that we've checked or approved the information or the source. You must use your own judgment when evaluating the content that you find.
 - f) **We don't give any guarantee about other websites, software or hardware, or their security or performance. We are not responsible for any loss caused by any failure or problem affecting any third-party websites.**
- 11 **Digital banking may sometimes be down**
- 11.1 **Digital banking might not always be available. Reasons for this include:**
- a) technical failure or problems with your device;
 - b) problems with a telecommunication or electricity service;
 - c) planned maintenance; and
 - d) other circumstances that are out of our control.
- 11.2 We aim to ensure minimum disruption to our digital channels. However, if our digital banking service is unavailable, you can register to receive up-to-date information about the status of our services.
- 11.3 **We are not responsible for any loss caused by any technical or other problems (interruption, malfunction, downtime or other failures that are out of our control) that might affect our digital channels.**
- 12 **Software and your devices**
- 12.1 **Use the latest update of the mobile banking app**
- You should only use the latest update of the mobile banking app. If you don't instal the latest update, the mobile banking app might not function properly. This means that you might experience security or data errors. We are not responsible for these errors or the consequences of these errors.
- 12.2 **Make sure your equipment and programs are suitable**
- You must use hardware (computer equipment) and software (computer programs) suitable for digital banking. If you don't, digital banking might not work properly, which could increase your security risks.
- 12.3 **You buy software at your own risk**
- a) If we offer software to you on or through digital banking, the licence agreement for that software is between you and the software's licensor (owner). We don't guarantee that any software is of good quality or suitable (right) for its purpose.
 - b) **You agree that, if the software licensor does not comply with the terms and conditions of the software licence agreement:**
 - iii. **we are not responsible for any loss that you may suffer; and**
 - iv. **you give up your right to claim against us for any loss that you may suffer.**
- 12.4 **You download apps and files at your own risk**
- We cannot guarantee that any file, download or application (app) through digital banking is safe to use on any device, nor can we guarantee that the system does not have software or data that could negatively affect a computer or device system. For example, it may have viruses, Trojans and other malicious (dangerous) software.**
- 13 **Our intellectual property**
- 13.1 **Defining intellectual property**
- In the terms of use, intellectual property means works of copyright, trademarks (statutory and common law), logos, images, multimedia, patentable inventions, patents, protectable design subject matter, designs, domain names and storage media, and includes applications, registrations and unregistered forms of these works and all other intellectual property rights (registered or unregistered) as well as the right to apply for these works in any country.
- 13.2 **We and our third-party licensors own the intellectual property rights**
- The intellectual property and all content on our digital channels belong to us or our third-party licensors. Nothing used in digital banking gives anyone the right to use our intellectual property without our written permission.
- 13.3 **You have a limited right to use the intellectual property**
- We give you the right to use the intellectual property to perform transactions on our digital channels. **You must not use the intellectual property for any other purpose.** This right starts when you start using our digital channels and ends as provided for in the terms of use. When your right ends, you must immediately stop using any intellectual property on our digital channels.
- 13.4 **Prohibitions on the use of intellectual property**
- You must not do any of the following in respect of our or our third-party licensors' intellectual property:
- a) copy or claim to have any rights to the intellectual property;
 - b) dispute or contest the validity of our ownership over the intellectual property; and
 - c) damage the reputation and goodwill associated with our intellectual property.
- 14 **Handing over rights and obligations (cession and assignment)**
- 14.1 **You must first get our consent in writing**
- a) You must not hand over (cede) your rights or delegate (assign) your obligations under the terms of use to any other person without first obtaining our consent in writing. (The person that you cede rights to is referred to as a 'cessionary' and the person that you assign obligations to is an 'assignee'.)
 - b) We alone may decide whether to grant or withhold our consent to a cession or assignment. If we grant our consent, we may update the terms of use to include extra rights for us or to impose extra obligations on the cessionary or the assignee. By accepting the terms of use, you agree to help us to negotiate changes with that cessionary or assignee if we consider the changes necessary.
- 14.2 **We don't need your consent to hand over rights or obligations**
- a) You agree that we may cede any or all of our rights or assign any or all of our obligations under the terms of use to any other person. We do not have to inform you of any cession or assignment unless the law requires us to do so.
 - b) The cessionary and the assignee have the right to exercise all our rights and obligations under the terms of use, including the right to process your personal information.
- 15 **If you don't comply with the terms of use**
- 15.1 **We may stop you from using digital banking**
- We may stop you from using digital banking if you don't comply with the terms of use and don't remedy the non-compliance within five business days after we've asked you to. Even if you do remedy it, we may still take steps against you, such as applying to court for an interdict (ban) or other order against you that prevents you from using digital banking.
- 15.2 **We may end our relationship with you**
- a) We may end our relationship with you and stop you from using digital banking by giving you written notice (Termination Notice). However, we don't have to give you notice, and we may suspend or terminate your access or use of digital banking immediately, if:
 - i. we believe or suspect that you are wrongly or unlawfully (illegally) using digital banking; or
 - ii. we must do this for legal reasons.
 - b) **We are not responsible to you for any loss you suffer if we cancel the terms of use or any other relationship that we have with you and if we specifically exclude or limit our responsibility in the terms of use.**
- 16 **Each term is separate**
- Each provision of the terms of use is separate. If a court or regulator finds that any term or condition is invalid or illegal or cannot be enforced, then removing that term or condition from the terms of use will not affect the provisions that remain.
- 17 **South African law governs the terms of use**
- The laws of the Republic of South Africa govern the terms of use, and the courts of South Africa have sole jurisdiction (the authority to hear and decide disputes).