Heartland online services terms of use

November 2023

HEARTLAND BANK

Acceptance of terms

By using any Online Services, you agree to be bound by these terms of use, as well as our Account and Service General Terms and Conditions and any other terms applying to a relevant account or service.

Further, you agree that you will not use, or permit to be used, Online Services for any purpose other than as intended.

Online Services Security

We provide the Online Services through Digital Banking or Mobile Apps. We regularly review developments in security and encryption and use strict procedures and security features to try to protect your personal information in our systems from misuse, loss and unauthorised access. We also encrypt your data travelling across the internet between our Online Services systems and your computer or device to protect and secure it. However, no communication over the internet can be guaranteed as completely secure. For that reason, whilst we endeavour to protect your personal information, we cannot guarantee the security of any personal information you transmit to, or from, the Online Services.

You are also responsible when using the Online Services to maintain the security of your personal information and to protect your Electronic Device from corruption or damage and these responsibilities are explained below.

If you have any concerns regarding the security of Online Services, feel free to contact us to discuss.

Your responsibilities

You are responsible for taking reasonable and appropriate steps to help maintain the security of your information, and protect your Electronic Device from corruption or damage, when using Online Services. You must ensure that:

a) your internet browser and Electronic Device are capable of supporting the encryption and other technical requirements of Online Services (as updated by us from time to time);
b) you establish and maintain (i.e. keep up-to-date) appropriate antivirus and other security software on your Electronic Device;
c) you do not open attachments or run software from untrusted or unknown sources;
d) you take any other reasonable steps necessary to protect your Electronic Device from being affected by viruses or anything else likely to corrupt or compromise your data;
e) you keep your User ID, password and pincode (as applicable) for Online Services secure at all times (including in accordance with our Account and Service General Terms and Conditions);
f) you do not allow any other person to access or open your Electronic Device using their Biometric Information where you have Biometric Information access enabled in the Mobile App;
g) you do not leave your Electronic Device unattended when logged on to Online Services, and you always log out correctly when you have finished using Online Services;
h) you do not use untrusted or shared Electronic Devices when accessing Online Services, such as computers at internet cafes;
i) you do not knowingly use an Electronic Device that contains software that has the ability to compromise passwords, pincodes and/or data (such as spyware);
j) you notify us immediately if:
    a. your Electronic Device is lost or stolen;
    b. you become aware that any other person is able to access or open your Electronic Device using their Biometric Information where you have Biometric Information access enabled in the Mobile App; and
    c. you become aware of any unauthorised use of Online Services provided to you;
k) you will regularly download updates to your Electronic Device's operating system software; and
l) you provide any relevant information, documents and attachments in the format and to the standards required by us for each transaction.

Biometric Information

You may choose to use Biometric Information to access the Mobile App via your Electronic Device instead of using a password or pincode. If you enable Biometric Information access to the Mobile App, then any other person whose Biometric Information is stored on your Electronic Device will also be able to access your accounts via the Mobile App. Accordingly, you must ensure that only your Biometric Information is stored on your Electronic Device where you have Biometric Information access enabled in the Mobile App.

You agree that you will be responsible for all actions on your accounts following a successful log-in into the Mobile App using Biometric Information from your Electronic Device.

Biometric Information is stored on your Electronic Device but is not made available to us, so we will not be able to verify the identity of any person who uses Biometric Information to access your accounts or the Online Services via an Electronic Device.

Availability

There will be times when we need to carry out planned maintenance on our Online Services. During these times some or all of the Online Services may be unavailable for a period of time and we will endeavour to give you as much notice as possible of the planned maintenance.

Heartland online services terms of use

November 2023

HEARTLAND BANK

In the event of an unplanned outage (for example, due to a technical fault or system error) we may be unable to give you advanced notice of the outage. However, we will make every effort to restore your services as quickly as possible.

There may also be times where you are unable to access our Online Services due to situations outside of our control (for example, internet connectivity issues or technical issues you're your devices). In these instances, we aren't liable for any consequence arising from the Online Services being unavailable.

We also aren't responsible if the device you use to access our Online Services doesn't work properly.

Our liability

To the maximum extent permitted by applicable law, we are not liable to you for any loss, harm or damage resulting from:

a) your failure to comply with these terms of use (and any other applicable terms);
b) us acting in accordance with these terms of use or our Account and Services General Terms and Conditions (and any other applicable terms);
c) anything that is caused by a matter outside our reasonable control (including the interception or hacking of data by unauthorised third parties);
d) any delay or loss of access to, or use of any Online Service at any time;
e) your failure to notify us of:
    a. the loss or theft of your Electronic Device or the actual or suspected disclosure of your password or pincode to another person; or
    b. when you know, or have cause to suspect, that another person may be able to access or open your Electronic Device using their Biometric Information where you have Biometric Information access enabled in the Mobile App;
f) your failure to disable access to the Mobile App via Biometric Information when you know, or have cause to suspect, that another person can access or open your Electronic Device and where you have Biometric Information access enabled in the Mobile App;
g) any faults, viruses, interruptions, machine failure, problems with a system or delays affecting Online Services; or
h) any unauthorised transaction made using Online Services where you have contributed to the loss, except (in each case) any loss, harm or damage arising as a direct result of our fraud or negligence.

Cancellation

You may cancel any Online Services at any time by contacting us.

Other things you should know

The use of Online Services may incur fees. Any applicable fee is set out in our Account and Service Fee Guide, which is available on our website.

You may also be charged by your mobile service operator for downloading, updating and/or using a Mobile App in New Zealand and overseas. We do not take any responsibility for any fees your mobile service provider charges you and if you have concerns about a fee you have been charged by your mobile service provider please contact them directly.

We can change these terms of use from time to time at our sole discretion.

We will give notice of any changes directly or indirectly by means of an electronic message, through our website, Digital Banking or Mobile App, through our branches, through the internet, through the media, or otherwise as we see fit and permitted by applicable law.

You acknowledge that:

a) we can also change the user requirements, application and operating system specifications, format or content of Online Services at any time without prior notice to you; and
b) there are risks associated with the use of Online Services (including, the risk that third parties may get unauthorised access to your personal information).

In these terms

Digital Banking means any website provided by us that allows access to banking and related services. **Mobile App** means any software application and/or web application that has been created to allow access to banking and related services and which suits portable electronic devices, including but not limited to, mobile phones.

Online Services means, as the context requires, Digital Banking and Mobile Apps.

We, us and **our** means Heartland Bank Limited and any of its related companies, and anyone who legally takes over any such company's responsibilities or rights (or both).