Terms & Conditions

Internet Banking

Effective 20 August 2019

bankfirst

invested in you

Summary of changes effective 20 August 2019

- New functionality has been enabled in Internet Banking which allows processing of international transfers. International Funds Transfers can be processed by a customer between their own Bank First account and an account at an international financial institution.
- The minimum age to register for SMS Security has been updated.

Contents

Terms and Conditions for Internet Banking

These Terms and Conditions contain information about Victoria Teachers Limited (ABN 44 087 651 769) trading as Bank First Internet Banking to help you make an informed decision when considering applying for our Internet Banking Service. Please read the Terms and Conditions carefully and retain a copy for future reference.
A copy of the Terms and Conditions are also available on our website or on request.
The relevant provisions of the Customer Owned Banking Code of Practice and the ePayments Code apply to our Internet Banking Service and we warrant that we will comply with these provisions.
Headings are for convenience only and do not affect the interpretation of these Terms and Conditions.

Internet Banking Features and Benefits

Internet Banking offers you the major features of banking in the convenience of a location that suits you, any time, day or night.
Bank First recognises that all information must remain confidential and your funds must be kept secure.
To do this we:

- Require customers to use unobvious passwords and to keep them secure.
- Require customers to use a One Time Password or secondary Password to add or change a Funds Transfer External payee, add or change a BPAY Biller,
- Require customers to use a One Time Password to add or change an NPP payee or create or manage a PayID.
- Require customers to use a One Time Password to add or change an International payee or create or manage an International Payee.
- Require customers to use a One Time Password to conduct an International Funds Transfer.
- Require customers to use a One Time Password to change their Visa Debit Card or Visa Credit Card personal identification number.
- Require customers to use a One Time Password or secondary Password if they are changing their personal contact details using Internet Banking or the SMS Alerts they wish to receive.
- Use Account timeout and blocking mechanisms.
- Only support the use of secure browsers that offer 128-bit encryption.
- Use firewalls, which protect your information and our systems.
- Regularly monitor activity logs for abnormalities.
- Send an Internet Banking confirmation email advice to the email address provided by you once a transaction has been successfully processed. You can disable this feature from within your Internet Banking settings if it is not required.

Internet Banking transactions are non-chargeable transactions. There is no limit to the number of free transactions you can make. Visit our website at **bankfirst.com.au** to access Internet Banking after registering.

With Internet Banking you can:

Transfer funds between selected Accounts internally and to other financial institutions (funds transferred externally, excluding International Transfers, Osko, and other NPP payments, are usually available at the receiving institution in 1-2 business days; this is dependent on the receiving institution and the time the transaction is initiated).

- Pay bills online using electronic transfers or BPAY on selected Accounts.
- Receive bills online via BPAY View.
- Check and print up to 12 months of your Account balances and transaction history.
- Download up to 12 months of transaction details.
- Transfer funds between selected Accounts internally and to other financial institutions (funds transferred externally, excluding Osko and other NPP payments, are usually available at the receiving institution in 1-2 business days; this is dependent on the receiving institution and the time the transaction is initiated).
- Transfer and receive Osko and other NPP Payments in near real-time.
- Create and Manage a PayID linked to your account.
- Transfer funds to international bank accounts.
- Create and manage International Payees.
- Obtain yearly interest earned details for taxation purposes (for current and previous financial year only).
- Change your Internet Banking password.
- Change your Visa Debit Card or Visa Credit Card personal identification number (PIN) using our Mobile Banking App; and ATM Card personal identification number using Internet Banking.
- Temporarily lock and unlock your Visa Debit Card and Visa Credit Card using our Mobile Banking App.
- Report your Visa Debit Card and Visa Credit Card as lost or stolen using our Mobile Banking App.
- Request a replacement Visa Debit Card and Visa Credit Card, where the card is damaged or not functioning correctly, using our Mobile Banking App.
- Open certain types of Accounts online.
- Personalise the screen settings to your individual requirements.
- Order a Personal Cheque Book or Deposit Book.
- Redraw funds available under any redraw facility on your loan where redraw has been activated.
- Change your phone, address and email details.
- Edit/delete BPAY Biller, External Funds Transfer and NPP payee details.
- Change the payment frequency for future dated payments.
- View, modify or delete future dated payments.
- View payroll details.
- Register your mobile phone for SMS Security and SMS Alerts.
- View Account information via your mobile phone if you have registered for SMS Alerts.
- View SMS Alerts in the event of specific transactions.
- Access Internet Banking using our Mobile Banking Service. Some functions will be unavailable when using the Mobile Banking Service.

Your Signatory will be able to perform the same functions with the exception of opening accounts.
Signatories are required to have their own Internet Banking access and login using their own login details. You are not to share your Internet Banking login and password details with your signatory.
Some of the above functions are unavailable when using the Mobile Banking Service and on certain types of Accounts. For example, you cannot make payments using the Internet Banking Service from a Term Deposit Account. See the general Account Terms and Conditions for features of each particular Account.
Before you use the Internet Banking Service, read the Terms and Conditions of Internet Banking carefully. You should follow the password and security guidelines detailed in clauses 2 and 3 of these Terms and Conditions below to protect against unauthorised access to your Accounts and information. You should also ensure that any Signatories or Authorised Account Viewers read the Terms and Conditions and follow the security guidelines.
If you or your Signatory fails to take the required security measures relating to passwords, or delays notifying us of any breach of the security of a Password or any misuse of the Internet Banking Service, you may be liable for any losses incurred. Liability for losses will be determined in accordance with clause 8 of these Terms and Conditions and the ePayments Code.

Terms and Conditions of Internet Banking

1 Definitions

In these Terms and Conditions:

- 'Account' means any Bank First Account or Accounts operated by you and accessible using the Internet Banking Service.
- 'Account Access Code' means the code shared amongst Signatories to a 'Two to Sign' Account and Authorised Account Viewers which provides limited Account access without an ability to perform transactions on the Account.
- 'Authorised Account Viewer' means any person authorised by you to view details of an Account using the Internet Banking Service.
- 'Authorised User' means you and any person you have authorised to operate your Account.
- 'Closed' in relation to a PayID, means a PayID which is removed from the PayID service, and unable to be used for NPP Payments.
- 'Funds Transfer External' means a transfer of funds between an Account and an account at another financial institution.
- 'International Funds Transfer' means a transfer of funds between an Account and an account at another international financial institution.
- 'Internet Banking Service', which incorporates our 'Mobile Banking Service' means the facility we provide to customers to enable them to receive information about Accounts, perform transactions and to transmit instructions to us electronically via the Internet.
- 'Locked' in relation to a PayID, means a PayID which we have temporarily disabled in the PayID service.

- 'Misdirected Payment' means an NPP payment erroneously credited to the wrong Account because of an error in relation to coding of the PayID or associated account information in the PayID, initiated by a Payer, who is a 'user', as that term is defined in the ePayments Code, which, as a result of the Payer's error is directed to the wrong Account.
- 'Mistaken Payment' means a payment, initiated by a Payer, who is a 'user', as that term is defined in the ePayments Code, which, as a result of the Payer's error is directed to the wrong Account.
- 'Mobile Banking Service' means the platform or application we provide to customers to enable them to access certain functions of our 'Internet Banking Service' via a Mobile Phone / device.
- 'Mobile Phone' includes any mobile device (such as a Personal Digital Assistant (PDA), Mobile Internet Device (MID) or tablet computer) which you (or, where the context requires, a Signatory or Authorised Account Viewer) use(s) to access our Mobile Banking Service and/or to send and receive SMS messages from the Bank in relation to the SMS Security and/or SMS Alerts.
- 'NPPA' means NPP Australia Limited.
- 'NPP' means the New Payments Platform.
- 'NPP Payee' means a customer who uses Osko or SCT services to receive payments.
- 'NPP Payments' means payments cleared and settled via the NPP.
- 'Bank' means Victoria Teachers Limited trading as Bank First.
- 'Organisation ID' means an identifier for a customer that is a business or organisation.
- 'Password' means your personal code, which provides access to the Internet Banking Service and to each Account you have nominated to be accessed by the Internet Banking Service, and includes:
  - Any secondary password which may be required to perform particular types of transactions such as payments to third parties or other Accounts with other financial institutions;
  - Each Signatory's personal code or secondary password which provides access to the Internet Banking Service in relation to one of your Accounts; and
  - Except in clause 2, a One Time Password.
- 'PayID' means an identifier you choose to use to receive NPP Payments.
- 'PayID Name' means the name we give you or the name selected by you (subject to our approval) to identify you to Payers when your PayID is used to make an NPP Payment.
- 'PayID Service' means the central payment addressing service offered through the NPP, which allows you to link your account to an easy-to-remember piece of information such as your mobile phone number, email address, ABN or Organisation ID.

- ‘PayID Type’ means the type of identifier you select for receiving NPP Payments, which may be your Mobile Number, Email Address, Australian Business Number (ABN) or Organisation ID.
- ‘PIN’ means the 4 to 9 digit Personal Identification Number used to access the Mobile Banking Application.
- ‘SCT’ means Single Credit Transfer; a NPP payment service.
- ‘SMS’ means Short Message Service.
- ‘SMS Security’ means the use of SMS messaging for authentication described in clause 14.
- ‘One Time Password’ means a computer-generated code sent via SMS to a registered mobile number which can be used for only one authentication process in order to initiate certain types of transactions. This password will not be accepted on second or following attempts.
- ‘Osko’ means the Osko payment service provided by BPAY allowing customers to make and receive payments in near real-time.
- ‘Osko Payment’ means a payment made by or on behalf of a Payer to a Payee using Osko, in near-real time with funds available almost immediately.
- ‘SMS Alerts’ is the opt-in service described in clause 15 which allows for customers to elect to receive an SMS message when one (or more) predefined events occur.
- ‘Signatory’ means you and any person you nominate as having authority to initiate a transaction on an Account individually or jointly with another Signatory.
- ‘Two to Sign’ means an Account with multiple signatories where two or more of those signatories must authorise transactions on an account.
- ‘Two to Sign Account Pending Authorisation’ means account transactions, not including Visa Card authorisations, that have been created and stored by one signatory and are awaiting approval by one or more further signatories.

Transactions made using the Internet Banking Service are governed by the Terms and Conditions of the Accounts being used. To the extent of any inconsistency, these Terms and Conditions prevail.

If any part of these Terms and Conditions is invalid, unenforceable or in breach of any law, it is to be interpreted as if that part is not included. The remainder of the Terms and Conditions continue in full force.

2 Password

- The Bank will provide you with access to the Internet Banking Service using a password that is issued to you when your application to use the Internet Banking Service is accepted and approved. Any Signatory granted access to the Internet Banking Service will be issued with a separate Password.

- You and your Signatory are required to change the initial password on first use of the Internet Banking Service. The new password must not relate to any readily accessible data such as your (or your Signatory's) name, date of birth, telephone number, driver's licence number or names of a friend, spouse, relative or pet.
- Each chosen password must not be an obvious combination of letters and numbers or one that can be guessed easily by someone else, and it must not be a series of consecutive or repeated numbers or characters.
- Each chosen password must not be the same as, or similar to, any other personal identification number you or your Signatory has for any other service provided or operated by us or any Account Access Code issued for a Two to Sign Account.
- For security reasons, you or your Signatory may be required to change a chosen password at any time.
- For additional security, we may require that a One Time Password or a secondary password be used for certain levels of access to the Internet Banking Service and to initiate certain types of transactions.

3 Keeping your passwords, PIN and mobile phone secure

You and each Signatory must keep your passwords and PINs (including any One Time Password) secret and take steps to prevent unauthorised use of passwords or PINs.

You or your Signatory must notify the Bank as soon as possible by phone on **1300 654 822** if you or your Signatory suspects another person knows the password or PIN or has used your password or PIN to your Account, or if you or your Signatory have registered for SMS Security and lost a registered mobile phone.

If you or your Signatory unreasonably delay notifying us, or if unauthorised access to your Account occurs through your or your Signatory's failure to guard against unauthorised use by complying with these Terms and Conditions, your liability for any loss arising from unauthorised transactions may increase.

To guard against unauthorised use, it is important that you and your Signatory:

- Do not tell anyone your password or PIN including family and friends.
- Do not respond to any request received, including any request which appears to be from the Bank, any other financial institution or Government agency, to provide a password or PIN.
- Do not keep any written record of any password or PIN. If you or your Signatory choose to store a password or PIN on your computer, you or your Signatory must ensure: - that the computer is kept secure with a further password and that the password is disguised so that it cannot be ascertained by anyone who gains access to it in its disguised form.

- Do not allow anyone to watch you or your Signatory enter the Internet Banking Service or observe or hear a password or PIN to your Account.
- Do not enter a password or PIN to your Account on any computer or mobile device where the security has been compromised and/or has Spyware, Malware or software that could allow your password, personal, or transaction details to be revealed.
- Exit immediately after you or your Signatory has finished using the Internet Banking Service by clicking the 'logout' button. You or your Signatory must not leave a computer or mobile device unattended while accessing the Internet Banking Service.
- Ensure you or your Signatory has access to your mobile phone when conducting a transaction using the Internet Banking Service.
- If you or your Signatory have registered for SMS Security and/or SMS Alerts , do not share a registered mobile phone with anyone.
- Lock a registered mobile phone with a password or code or take other measures to stop unauthorised use of the Internet Banking Service using the mobile phone.
- Promptly delete SMS messages you or your Signatory have sent to or received from the Bank from a registered mobile phone.

Please note when registered for SMS Security you are responsible for taking reasonable and appropriate security measures in relation to your mobile phone.

You are also responsible for ensuring that any Signatories who are registered for SMS Security take reasonable and appropriate security measures. The Bank has no control over who can access the information supplied by the Bank to your or your Signatory's mobile phone.

We will issue at least annually a clear, prominent and self-contained statement summarising the password security guidelines.

4 Two to Sign Accounts

Each account holder or signatory will be issued with their own individual account login and password. This account login and password must be used to load and authorise transactions via the Internet Banking Service. You must ensure that you keep your password secure in accordance with clauses 2 and 3.

Signatories and Authorised Account Viewers may have view only access (no transactions can be made) by entering the account number and Account Access Code for the 'Two to Sign' account. This Account Access Code is common to all Signatories and Authorised Account Viewers.

Account Payments

Where an account has signing instructions of 'Two to Sign', signatories may load and authorise payments via the Internet Banking Service by using their own individual account login and password.

Where there are multiple signatories on a 'Two to Sign' account, the loading and authorisation by any two signatories will be accepted and the transaction processed. Where the account operation requires a minimum of three (or more) signatories to sign, the loading and authorisation by any three (or more) signatories will be accepted and the transaction processed.

Once a transaction has been established by the first signatory it will await approval within the Internet Banking Service. The transaction will be stored as a 'Two to Sign Pending Authorisation' and will not be successfully processed until it has been subsequently authorised by a further signatory(s).

Authorised signatories will be advised on the Internet Banking homepage of any transaction awaiting authorisation within Internet Banking.

Each signatory is required to register for either a Funds Transfer Password or SMS One Time Password. The Funds Transfer Password or SMS One Time Password is personal to the Signatory. In order To complete a 'Two to Sign Pending Authorisation' the signatory authorising the transaction will be required to enter either the Funds Transfer Password or SMS One Time Password.

If a 'Two to Sign Pending Authorisation' has not been fully authorised within 7 days from the date the payment was loaded it will be automatically deleted.

In order to revoke the authority given to a Signatory or Account Viewer, or to update the authorised signatories on the Account, you must complete and submit to us a Change of Signatory Authorisation in the form required by us.

5 Internet Banking Service Fees and Charges

5.1 You must pay the Bank's standard fees and charges relating to the SMS Alerts service in accordance with this clause 5.

5.2 When you use the SMS Alerts service: SMS Alerts fees are charged on a monthly basis. SMS Alerts fees accrue until the end of the month in which they are incurred and are debited from your Account balance in the first week of the following month and when the Account is closed. SMS Alerts fees will be debited to your primary Account (usually your Transaction Account), regardless of whether the information provided or requested through an SMS Alert relates to that primary Account.

5.3 The amount and nature of the standard fees and charges relating to use of the SMS Alerts service by you are set out below. These fees are subject to change.

Fee and charge amount:
SMS Alerts $0.25 per SMS

5.4 A telecommunications provider may also impose charges on you or your Signatory in respect of SMS messages. Any such charges are your or your Signatory's responsibility and any matters regarding these charges should be raised with the telecommunications provider.

5.5 If the fees and charges for the SMS Alerts service cause the relevant Account to become overdrawn, the Bank may require you to pay the fees immediately.

5.6 If you close your Account, the Bank will select another Account which you have with the Bank to which SMS Alert fees may be debited. If the Bank determines there is no satisfactory Account, the Bank may immediately cancel the availability of the SMS Alerts service to you until such time as you pay the Bank the fees in a manner acceptable to it.

5.7 For transactions on certain Accounts, fees and charges may be payable under the Terms and Conditions governing those Accounts where the transactions are initiated by our Internet Banking Service. A payment return fee applies when a transaction is processed to an external Account and is rejected. The fee is applied per item.

6 Responsibility for Signatories and Authorised Account Viewers

- You must ensure that all Signatories and Authorised Account Viewers are aware of these Terms and Conditions and you are responsible for ensuring that they protect the security of the passwords, Account Access Codes, and mobile phones in accordance with these Terms and Conditions.
- You are responsible and liable for all actions by the Signatories and Authorised Account Viewers in relation to the Account.
- You must ensure the Signatories and Authorised Account Viewers do not do or omit to do anything which contravenes your obligations under these Terms and Conditions.
- You must also ensure that Signatories and Authorised Account Viewers do not share passwords with each other or with any other person.

7 Transaction limits

Use of the Internet Banking Service is subject to transaction limits. These may be imposed by us or by other parties involved in any transaction. These include:

- The maximum amounts which can be transferred in any day.
- The maximum number of transactions in any day.
- The maximum amounts for bill payments.

The following daily transaction limits via our Internet Banking Service apply, unless otherwise arranged by you or altered by you via the Internet Banking Service:

For External Transfers

A maximum daily limit of $14,000 applies to each account, for example, if you have three accounts accessible via the Internet Banking Service, a combined $42,000 would be available across all three accounts. The $14,000 maximum limit is a single account limit irrespective of the number of Authorised Signatories to an account. The following sub-limits also apply to external transfers per account:

- BPAY - $10,000.
- External Transfers - $2,000.
- NPP - $2,000.

Loan Redraw is captured by the above sub-limits.

For Internal Transfers

There is no maximum daily limit for transfers between Accounts that are linked under the same Internet Banking Login. Any amount may be transferred up to the available Account balance or credit facility.

Our agreement to increase any of these limits is at the Bank's discretion and may be subject to the requirement that additional security measures be taken, for example, a secondary password be used to effect transactions.

For International Funds Transfer

A maximum daily limit of $5,000 applies to each account. This limit is separate from the External and Internal transfer limits. For example, if you conduct a BPAY transaction for $10,000, an External Transfer for $2,000 and a NPP transfer for $2,000, your International Funds Transfer limit would not be effected and you have a remaining $5,000 available for this form of transaction.

8 Liability for unauthorised use

8.1 You are liable for all transactions initiated by you or any Signatory. You are also liable for all transactions initiated by any other person to whom you or any Signatory have disclosed or facilitated the disclosure of any password or PIN in breach of these Terms and Conditions.

Where a transaction is initiated by the use of the correct password or combination of passwords or PIN, we shall take it that you have instructed us to process the transaction and, subject to these Terms and Conditions, you shall be liable for the transaction and any fees and charges incurred in respect of the transaction.

You must therefore ensure that each password or PIN is kept secure and confidential by you or any other Signatory to whom we issue a password on your request (including One Time Passwords under the SMS Security service). You must ensure that you and each Signatory complies with the security requirements described in clauses 2 and 3.

8.2 You must notify us immediately upon you or any Signatory becoming aware of:

a) The security of a password or PIN being breached (including any One Time Password and when any item on which a Password is recorded is lost or stolen); or

b) Any other misuse of the Internet Banking Service; or

c) The loss or theft of any mobile phone, the number of which has been registered for SMS Security; or

d) The change of mobile phone number, where the number replaced was registered for SMS Security.

If any of these things occur, you must notify us as soon as possible by calling **1300 654 822**.

8.3 You will be liable for losses arising from unauthorised transactions entered into before you notify us that the security of the password or PIN has been breached or the Internet Banking Service has been misused where we establish on the balance of probability that you contributed to the losses:

a) By failing to choose and protect the password or PIN in accordance with clauses 2 and 3 or otherwise acting with extreme carelessness in failing to protect the security of the password; or

b) By unreasonably delaying notification to us of the security of the password or PIN being breached or the Internet Banking Service being misused.

Subject to the Terms and Conditions governing the relevant Account debited for the unauthorised transaction, your liability under this clause will not exceed the lesser of:

a) The daily transaction limit applicable to the Internet Banking Service for each day or part thereof during which the transaction occurred prior to notification to us; or

b) The balance of the relevant Account or Accounts agreed to be accessible by Internet Banking (including any pre-arranged credit limit) at the time of the unauthorised transaction.

Where it cannot be established that you or your Signatory contributed to losses:

a) By failing to choose and protect the password in accordance with clauses 2 and 3 or otherwise acting with extreme carelessness in failing to protect the security of the password; or

b) By unreasonably delaying notification to us of the security of the password being breached or the Internet Banking Service being misused.

Your liability for such losses will not exceed the lesser of:

a) $150;

b) The balance of the relevant Account or Accounts agreed to be accessible by Internet Banking (including any pre-arranged credit limit) at the time of the unauthorised transaction; or

c) The actual loss at the time we are notified of the breach of security of the password or of the misuse of the Internet Banking Service capped for each day on which a loss is incurred at the applicable daily transaction limits.

8.4 You will not be liable for losses arising from unauthorised transactions where it is clear that you have not contributed to that loss. You are not liable for loss that:

a) Is caused by the fraudulent or negligent conduct of any of our employees or agents or the employees or agents of a company or person in the network on which the Internet Banking Service is provided;

b) Results from unauthorised transactions involving a password which is forged, faulty, expired or cancelled;

c) Occurs before you have received your account number or initial login password; or

d) Results from unauthorised transactions after you have notified us that the password or PIN security has been breached or the Internet Banking Service has been misused.

9 Mistaken and Misdirected Payments

- Mistaken payments will be investigated in accordance with the ePayments Code and/or NPP Regulations, whichever is applicable.
- If the Bank is satisfied that a Mistaken Payment or Misdirected Payment has been made to your Account by another party, we may be able to reverse that payment, even if you have not authorised the Bank to do so.
- Where we and the sending financial institution determine that an NPP Payment made to your Account is either a Mistaken Payment or a payment made in error, we may, without consent, and subject to complying with other applicable Terms & Conditions and NPP Regulations, deduct from your Account, an amount up to the original amount of the Mistaken Payment or payment made in error. A payment made in error includes a fraudulent payment, an over payment, or a Misdirected Payment. We will notify you if this occurs.
- You will be liable for losses arising from a Mistaken Payment or Misdirected Payment you or your Signatory has made to a third party where it is not possible for the Bank to recover those funds from the unintended recipient.

10 Accounts

You should check your Account statements and records carefully. If you believe a transaction is wrong or unauthorised you should telephone us immediately on 1300 654 822.

11 PayID

About PayID

11.1 The PayID service is the NPP Payment addressing service that enables payers to make NPP Payments to payees using an alternative identifier instead of Account details.

11.1.1 Before you can create your PayID to receive NPP Payments into your Account, you must satisfy us that you either own or are authorised to use your chosen PayID and have an eligible Account.

11.1.2 You must be registered for SMS Security to be eligible for PayID.

11.1.3 We will use processes to establish your ownership and authority to use a chosen PayID by means of SMS Security or Email Verification Code.

11.1.4 PayID is an optional service for customers. Whether you choose to create a PayID for your Account or not, you and each Authorised User, may use a payee's PayID to make particular types of NPP Payments to the payee from your Account provided that:

(a) Bank First and the payee's financial institution support NPP Payment service;

(b) The payee's account is able to receive the particular NPP Payment; and

(c) The PayID is not locked.

Choosing a PayID and PayID Name

11.2 Bank First supports the use of the following PayID Types:

a) Mobile number

b) Email Address

c) Australian Business Number (ABN)

d) Organisation ID

We may update this list from time to time.

11.2.1 You can create a PayID as long as it is a supported PayID Type. Some PayID Types, for example Organisation IDs, are restricted to business customers and organisations and can only be created by contacting us.

11.2.2 You must satisfy us that you own or are authorised to use your chosen PayID before you can use it to receive NPP Payments. This means we may ask you to provide evidence to establish this to our satisfaction, whether you are already registered for any other mobile or online banking or online payment services with us or not.

11.2.3 Your PayID Name may be displayed to payers who send NPP Payments to you. You must ensure your contact details are up to date with the bank, for example, name, mobile phone number and email address. At the same time you create your PayID, we will:

(a) automatically assign a PayID Name for display to payers; or

(b) select an alternative PayID Name, such as your business name, for display.

11.2.4 We will not permit selection of a PayID Name that is likely to mislead or deceive a payer into sending you NPP Payments intended for another payee, or which for any reason is inappropriate.

Creating your PayID

11.3 By creating your PayID you acknowledge that you authorise:

a) us to record your PayID, PayID Name and Account details (including full legal account name) in the PayID service;

b) NPP Participants which are payers' financial institutions to use your PayID information for the purposes of constructing NPP payment messages, enabling payers to make NPP Payments to you, and to disclose your PayID Name to payers for NPP Payment validation.

11.3.1 You can create a PayID for receiving NPP Payments through a Bank First online banking service that supports PayID creation. We will not create a PayID for you without your prior consent.

11.3.2 You may choose to create more than one PayID for your Account.

11.3.3 If your Account is a joint account, you and each other joint account holder can create a unique PayID for the Account.

11.3.4 If you have Authorised Users on your Account, each Authorised User may create a unique PayID for the Account.

11.3.5 Once a PayID is created and linked to your Account, it may not be used in relation to any other account with us or with any other financial institution. See clause 11.4 for details on transferring PayIDs.

11.3.6 The PayID service does not support duplicate PayIDs. If you try to create a PayID for your Account which is identical to another PayID in the service, you will see the following message: "*The requested PayID is already being used elsewhere*". You can contact us on **1300 654 822** to discuss duplicate PayIDs however we cannot disclose any personal information in connection to the use of a duplicated PayID.

Transferring your PayID to another Account

11.4 You can transfer your PayID to another account with us or to another financial institution by going to the 'Manage PayID' function in one of our online banking channels.

11.4.1 A transfer of your PayID to another account with us will generally be effective immediately, unless we notify you otherwise.

11.4.2 A transfer of your PayID to another financial institution is a two-step process initiated by you and completed by the registering financial institution.

11.4.3 Until the transfer is complete, payments to your PayID will continue to be directed to your associated Account with us. If the other financial institution does not complete the transfer within 14 days, the transfer will be deemed to be ineffective and your PayID will remain with your current Account.

Transferring your PayID from another Financial Institution

11.5 A PayID registered to another financial institution can be transferred to your Account held with us by commencing the transfer process with the other financial institution.

Closing a PayID

11.6 You may close your PayID at any time using the 'Manage PayID' function in the relevant online banking service. Closing a PayID results in removal of your PayID from the PayID service.

11.6.1 You must notify us immediately if you no longer own or have authority to use your PayID.

11.6.2 We may close your PayID where:

(a) We close your account

(b) We are not satisfied that you own or are otherwise authorised to use that PayID; or

(c) We reasonably suspect that the PayID is or has been used for a fraudulent purpose; or

(d) Your PayID has remained inactive or locked for a period that we reasonably consider to be excessive; or

(e) We are required to do so by law or by the operator of the New Payments Platform.

Locking and Unlocking a PayID

11.7 We monitor PayID use to manage PayID misuse and fraud. You acknowledge and consent to us locking your PayID if we reasonably suspect misuse of your PayID or use of your PayID to procure NPP Payments fraudulently.

11.7.1 You will not be able to transfer your PayID or receive payments addressed to your PayID while your PayID is locked.

Payments to your PayID

11.8 We will ensure that your PayID and Account details are accurately recorded in the PayID service.

11.8.1 Not all accounts and payment types support payment to a PayID. The ability for a payer to pay to your PayID depends on the payer's financial institution and on the type of payment to be made. In some cases you may need to provide your BSB and account number to the payer.

Making Payments to a PayID

11.9 When you enter the PayID in the payee field of the relevant online banking or mobile service, we will check to confirm that the PayID has been registered in the PayID service. Where it has, we will display to you on screen PayID Name attached to that PayID. You must check that name displayed matches the person that you intend to pay. If you do not recognise the name or the name does not match who you intend to pay, you should contact your intended payee to confirm that all details are correct before proceeding to make payment. Incorrect details could result in a payment to the wrong account and may result in loss of your funds.

11.9.1 When you direct a payment or other message to a PayID connected to a joint account, the other account holders may be able to see the messages and notifications associated with the payment.

How we process future dated payments to a PayID

11.10 We may attempt to make the payment at any time on the scheduled payment date. You should ensure that you have sufficient funds available throughout the day to satisfy the payment. We may decline to process the payment if, at the time we try to make the payment you don't have sufficient funds in your account.

11.10.1 On the scheduled payment day, before we try to make the payment we will check the PayID service to confirm whether the PayID is still registered and whether there has been a change in the name attached to the PayID since the time you established the payment. We won't be able to process the payment if the PayID is no longer registered or is locked or if the name attached to the PayID has changed. You should check the payment status on the scheduled day to confirm successful processing.

Privacy

11.11 By creating your PayID you acknowledge that you consent to our recording of your PayID, PayID Name and account details in the PayID service to enable payers to make NPP Payments to you, and to the extent that such recording and use constitutes a disclosure and use of personal information within the meaning of the Privacy Law, consent to that disclosure and use.

We are obliged to disclose your personal information (PayID Name and PayID) to third parties including NPPA for the purposes of PayID registration and to other NPP Participants for the purposes of enabling NPP Payments to be sent and received and for reasonable secondary purposes that include payment investigations.

Where you hold a joint account, other account holders may be able to see messages and notifications associated with payments and other messages addressed to your PayID.

To the extent that the creation and use of the PayID Record constitutes a disclosure, storage and use of your personal information with the meaning of the Privacy Law, you acknowledge and agree that you consent to that disclosure, storage and use.

12 Osko

About Osko

12.1 Bank First subscribes to Osko under the BPAY Scheme.

12.1.1 Osko is a service that allows customers to make and receive payments in near real-time, 24 hours a day 7 days a week.

12.1.2 We offer the service to all our customers who satisfy the requirements set out in these Terms & Conditions.

12.1.3 All eligible accounts can receive Osko payments. An Osko payment can only be sent via Internet Banking, Mobile Banking and Mobile App.

12.1.4 We will notify you if, for any reason, we are no longer able to offer you Osko. If we are no longer able to offer you Osko services, you will not be able to send or receive Osko payments.

12.1.5 Where we are able to do so we will tell you:

(a) If there are any delays in processing transactions; and

(b) When your transaction is completed.

How to use Osko

12.2 You can make Osko payments to a PayID or a BSB and Account Number, provided that the account that you are paying can receive Osko payments. The payee's ability to receive the payment is at the discretion of their financial institution.

12.2.1 You should ensure that all information you provide in relation to any Osko payment is correct as we will not be able to cancel an Osko payment once it has been processed.

12.2.2 Osko payments will be processed immediately with exception to instances where there are insufficient funds in the account at the time of payment, including any future payments, or as per clause 20.

Suspension and Termination

12.3 We may suspend your ability to make Osko payments or other NPP payments at any time if we suspect that you, or someone acting on your behalf:

(a) Act fraudulently or are suspected of fraudulent behaviour.

(b) Use Osko in a manner that will or is likely to affect our ability to continue providing Osko to our customers.

(c) Breach any obligation under these terms and conditions which is incapable of remedy.

(d) Suffer an insolvency event.

12.3.1 We may also make the service temporarily unavailable for the purpose of performing system maintenance or upgrades.

12.3.2 We may immediately terminate and/or suspend your participation in Osko by notifying you if our membership to the BPAY Scheme or our subscription to Osko is suspended, ceases or is cancelled for any reason.

Privacy

12.4 In order to provide you with services under Osko, we may need to disclose your personal information to BPAY and/or its service providers. If we do not disclose your personal information to BPAY or its service providers, we will not be able to provide you with services under Osko.

Accordingly, you agree to our disclosing to BPAY, it's service providers and such other participants involved in Osko such personal information relating to you as is necessary to facilitate the provision of Osko to you.

We only collect, use, disclose or store your personal information in accordance with the requirements of the Privacy Act 1988 and our Privacy Policy.

We will keep any information you provide to us confidential. We will make reasonable efforts to keep any such information that we have about you secure and to ensure that any of our employees or agents who have access to information about you do not make any unauthorised use, modification, reproduction or disclosure of that information.

You must notify us if any of your personal information changes.

13 International Funds Transfers

13.1 'Purchaser' means the customer applying for an International Funds Transfer. The 'Foreign Exchange Provider' means American Express International Inc – ABN 15 000 618 208.

13.2 The Bank will process requests for International Funds Transfers to a specified international bank account, provided sufficient funds are available in your account.

13.3 The Bank shall not be liable for losses arising directly or indirectly from circumstances beyond its control, including the failure of any other financial institution to properly process the International Funds Transfer. The Bank will not be liable for any loss or damage incurred directly or indirectly as a result of acting on this instruction in good faith and without negligence.

13.4 Indicative exchange rates are available by contacting the Bank. The exchange rate provided to the Bank is at the absolute discretion of its Foreign Exchange Provider. The exchange rate applied to the International Funds Transfer is the exchange rate that is current at the time of processing and therefore may vary from the exchange rate at the time

of submitting an application or a rate previously advised. As correspondent banks and overseas financial institutions may deduct commissions or fees from the money transferred, the payee may receive less than the amount sent.

13.5 This payment is undertaken at the Purchaser's risk. The Foreign Exchange Provider and their agents accept no liability whatsoever for any delay, mistake, or omission which may occur during transmission, processing by the recipient bank or their agents, or from failure to identify the Payee. The bank shall not be responsible for payment to the payee by the payee's financial institution and reserves the right to charge you for the cost of correspondence relating to International Funds Transfer enquiries.

13.6 Once an application has been processed, it may not be possible to reverse the transaction without the co–operation of the payee. The Bank shall not be liable for the failure of any cancellation or amendment to an instruction being successfully effected.

13.7 Upon reversal of an International Funds Transfer, due to cancellation or return of the instruction, any refund will be calculated at the foreign exchange rate prevailing at the time and is determined at the absolute discretion of the Bank's Foreign Exchange Provider. The exchange rate prevailing at the time may result in an exchange rate loss to the purchaser.

13.8 In the event of cancellation or amendment of an International Funds Transfer instruction, the Bank may charge or debit the customer's account with a cancellation or amendment fee. The amount of such fee will depend upon the amount of any fees imposed upon the Bank by its Foreign Exchange Provider.

13.9 The Purchaser agrees to pay all charges and liabilities imposed upon the Bank by its Foreign Exchange Provider or its correspondents and agents in connection with an application and the carrying out of the Purchaser's instructions.

14 Use of Internet Banking Service

We will endeavour to effect transactions on your Account that are received via the Internet Banking Service, provided there are sufficient funds available in your Account and any applicable transaction limits have not been exceeded. However, you are responsible for ensuring that the intended recipient receives any payments made using the Internet Banking Service. We will not have any responsibility or liability for any refusal or omission to initiate or complete any transaction, or to do so by any particular time, or for any omission to follow any transaction instructions. At busy times, the Internet Banking Service may be unavailable, and we have no liability in respect of that unavailability.

Some financial institutions process payments using BSB and Account number only and may not correlate this information with the account holder's name. It is therefore essential that you input the correct BSB and Account number to ensure that the payment reaches its intended destination. Funds sent using incorrect details may not be recoverable.

Bank First is not liable for payments that are made to an incorrect account where the Account details or PayID that you provide are incorrect.

We have set a monetary limit on the transactions that can be carried out using the Internet Banking Service and on the number of transactions able to be made in any period. Limits or restrictions may vary depending on the type of transaction or we may modify the limits or restrictions at any time.

The Internet Banking Service will be subject to continual upgrading and enhancement. Accordingly, we may need to modify, enhance, cancel, or withdraw the Internet Banking Service at any time.

You may request in writing, at any time, that we withdraw your access to the Internet Banking Service or the access given to any Authorised Account Viewer or Signatory. You will remain responsible for any transactions made on your Account using the Internet Banking Service until the request has been received and processed by us.

15 Alerts

15.1 Who can register for Alerts? You and each Signatory are eligible to apply to register for the Alerts service, provided that:

a) You have an Account which is eligible for SMS Security (as we determine from time to time);

b) The person registering has an eligible mobile device capable of SMS messaging.

15.2 **Alert Delivery Options**

You and your Signatory can opt to receive Alerts via SMS or Email. Alerts sent via SMS will incur a fee in accordance with clause 5.3.

If you opt to receive Alerts via SMS, the person registering must provide a valid mobile phone number and have an eligible mobile device capable of SMS messaging.

Alerts sent via email are free of charge.

15.3 **How to register**

You and your Signatory can register for Alerts through our Internet Banking Service.

During registration, you or your Signatory will be asked to:

a) Provide the mobile phone number of a mobile device capable of SMS messaging.

b) Select options to receive Alerts via SMS and/or Email.

15.4 **Receiving Alerts**

Once you and your Signatory have registered for Alerts and have chosen the Alerts you wish to receive, the Bank will send messages via SMS or Email containing information about certain Accounts with the Bank to the registered mobile phone number or email address you or your Signatory provided in the registration process. You can opt out of the Alerts Service at any time by deselecting the Alerts options through Internet Banking.

16 SMS Security Service

16.1 **How to register**

You and your Signatory will need to contact us during business hours on 1300 654 822 to register for this service. We will approve a request to register for the SMS Security services in accordance with clause 16.1 at our discretion.

Please note that you and your Signatory must be aged 12 years or older to register a mobile phone for this service.

16.2 **SMS Security**

Once registered, you and your Signatory will be required to supply a One Time Password each time certain functions using the Internet Banking Service are performed. This One Time Password will be sent to the mobile phone number provided in the registration process.

If at any time you and your Signatory wish to deregister from SMS Security, contact us at 1300 654 822. You or your Signatory will be deregistered from receiving SMS Alerts at the same time as deregistering from SMS Security.

16.3 We may at any time add to, remove, change or impose restrictions on the SMS Security functionality in any respect and without limitation.

17 Mobile devices

17.1 Not all mobile devices may be capable of accessing and using the Mobile Banking Service or the SMS Security and SMS Alerts service.

You and your Signatory are responsible for using, having or obtaining a compatible mobile device in connection with any use of the service.

Bank First is not responsible for any inability of a mobile device to access the service or any loss or damage to a mobile device resulting from your or your Signatory's access or use or attempted use of the service.

17.2 If you or your Signatory travel outside Australia, you may still have access to the Mobile Banking and SMS services. You or your Signatory should check with the telecommunications provider that the mobile device will be able to use the internet and SMS network in those countries in which you or your Signatory are travelling and that the mobile phone number registered for the SMS service can be retained.

17.3 Any conditions of use and charges relating to a mobile device are your or your Signatory's responsibility.

17.4 If you or your Signatory believe a registered mobile phone is lost, stolen or damaged please refer to clause 8 'Liability for unauthorised use' for the action to take to limit your liability.

18 Opening Accounts

The Bank may allow you to open certain types of Accounts using the Internet Banking Service.

- Christmas Club Account.
- Bonus Saver Account.
- Online Saver Account.
- Budget Savings Account.

19 System malfunction

We will make all reasonable efforts to ensure that the Internet Banking Service is available 24 hours a day, seven days a week. However, the Bank is not liable:

- For any breakdown in the Internet Banking Service for any reason whatsoever or any inability to access the Internet Banking Service;
- For any corruption of data and any breakdown, interruption or errors caused to a computer as a result of using the Internet Banking Service;
- For any corruption of SMS data and any SMS gateway breakdown or interruption or errors caused to your mobile device as a result of a telecommunications service provider; or
- For failure or delay in delivering a One Time Password, and/or SMS Alerts as a result of the failure of a telecommunications provider or its network.
- You will not be liable for losses caused by our system or equipment failure in the completion of a transaction. This limitation on your liability does not apply to the operation or failure of any external system or equipment including any system or equipment used by you or on your behalf.

20 Changes to Terms and Conditions of Internet Banking

We may vary these Terms and Conditions subject to giving you notice in accordance with this clause.

For changes being:

- An increase of fees and charges including the introduction of new fees and charges; or
- An increase of your obligations or change of transaction limits.

We will give you not less than 30 days advance written notice. For changes to Government charges, we will give you written notice no later than the time we next communicate with you. For all other changes, we will give you notice by advertisement in the national or local print media or a customer newsletter or Account statement or other notice to you at the following times:

a) If we reasonably believe that the change is not adverse to your interests and we would not expect you to be concerned about a delay in receiving notice, no later than the time we next communicate with you; and

b) Otherwise, not later than the time the change takes effect.

21 Blocking and delays on accounts and payments

21.1 a) We may be required by law, a Government agency or regulatory authority and/or international treaties, sanctions to which Australia is a party (referred to as Authorities), or our policies, not to initiate or complete a transaction on your Account, initiated by you or initiated on your behalf.

b) Further, we may, from time to time, require further information from you, or a person authorised by you to assist us in meeting our obligations under the law and our policies.

c) We may also be legally obliged to disclose information about you to Authorities, other financial institutions, or our service providers without giving you any notice.

21.2 You and any person authorised by you agree not to begin or undertake a transaction that causes you to breach any Australian law, or law of any other country.

21.3 You agree we can:

a) Screen payments, transactions and other communications initiated or sent by you or on your behalf; and

b) Block and/or delay payments, transactions and communications, including blocking permanently, due to screening or our obligations under this clause.

21.4 Further, you also agree as a consequence of our obligations under this clause that we may in our absolute discretion refuse paying, initiating or completing any transaction for you, or on your behalf without any obligation to give you any notice or warning.

21.5 As far as it is permissible under law and under any relevant code of conduct which we are, or choose to be bound by, we are not liable to you, or others for:

a) Any direct, indirect or consequential loss, or

b) Damage, loss of profit or opportunity which arises as a result or consequence (direct or otherwise) of:

i. Any action, inaction, delay, failure to pay; or

ii. Delay in communications; or

iii. Any other obligations and duties that we may have to you, or others, as a result of us performing, not performing, or part performing any duties or obligations we may have under this clause.

22 Statements

22.1 In lieu of receiving paper statements you may be able to elect to receive electronic statements (eStatements) for your accounts via the Internet Banking service. If you choose to receive eStatements, we will no longer send you paper statements for your accounts.

You may however, elect to revert back to paper statements at any time. If you choose to revert back to paper statements, where you had also opted to receive eNotices, you will also be reverted back to paper notices. You can do this via the Internet Banking service, by visiting one of our branches or by calling our Member Contact Centre during business hours on **1300 654 822**.

Where you have elected to receive eStatements we will promptly send you an email or SMS notification to your nominated email address or mobile phone number advising you that your eStatements are available via the Internet Banking service. You cannot opt out of receiving these notifications however you can change your nominated email address or mobile phone number at any time via Internet Banking, by visiting one of our branches or by calling our Member Contact Centre during business hours on **1300 654 822**.

It is your responsibility to:

a) Keep your email address and mobile phone number current and advise us as soon as possible if these change;

b) Check your emails and SMS regularly for eStatement notifications;

c) Promptly log in to Internet Banking to view your eStatements once you have received notification; and

d) Advise us if you have any problems accessing your email or SMS notifications or Internet Banking.

Where you have received an eStatement, we will provide you with a paper copy of that statement if you request one within 6 months of the receipt of the eStatement (a fee may apply - refer to Terms & Conditions Part B: Fees and Charges).

22.2 The Bank maintains the right to withdraw from sending electronic statements at any time.

23 Notices

23.1 By providing an email address in connection with Internet Banking, you agree that we may send you notices in relation to these Terms and Conditions by addressing them to that email address, or any other email address you notify to us from time to time for that purpose. You also agree that we may give you notices of changes to these Terms and Conditions by displaying them on the Internet Banking service.

23.2 Where you have elected, and where permitted by law, we may also transmit any notice or document to you by any form of electronic communication (eCommunication) which you nominate to us by, for example, providing us with a fax number, email address or mobile phone number for SMS. You can only elect to receive eCommunications if you have also elected to receive eStatements.

23.3 Where you have elected to receive eCommunications we will no longer send you paper notices.

You may however, elect to revert back to paper notices at any time. If you choose to revert back to paper notices, you will also be reverted back to paper statements. You can do this via the Internet Banking service, by visiting one of our branches or by calling our Member Contact Centre during business hours on **1300 654 822**.

It is your responsibility to:

a) Keep your email address and contact details current and advise us as soon as possible if these change;

b) Check your emails and SMS regularly for eStatement notifications;

c) Advise us if you have any problems accessing your email or SMS notifications or Internet Banking.

23.4 The Bank maintains the right to withdraw from sending eCommunications at any time.

23.5 Notices or documents sent by fax shall be taken to be received at the time indicated on the fax transmission report generated by the transmitting fax machine. Notices or documents sent by email or SMS shall be taken to be

received at the nominated address or phone number at the time they enter the information system of the nominated address or phone.

24 If You Have a Complaint about Internet Banking

A Complaint and Dispute Resolution Guide is available to all customers in our branches, on our website and by request. The Guide informs customers about how to lodge a complaint, including who to contact and how the Bank aims to deal with the complaint. Customers who lodge a complaint will be offered this guide.

If your complaint relates to this product, you should first contact one of our Member Service Consultants on **1300 654 822**.

If your complaint cannot be resolved by the Member Service Consultant, you may request to use our Internal Dispute Resolution procedure. Your complaint will be referred to an appropriately trained Consultant within the Bank, who will register your complaint and advise you of our process to deal with your complaint.

In the event that you are not satisfied with our resolution of your complaint through our Internal Dispute Resolution procedure, you are entitled to have your dispute considered, free of charge, by our External Dispute Resolution procedure. If you wish to use this procedure, please contact the Australian Financial Complaints Authority on 1800 931 678.

Privacy Information

Your personal information will be treated strictly in accordance with our Privacy Policy set out on our website at **bankfirst.com.au** and available on request. At any time you may gain access, upon request, to the information we hold about you in accordance with the Australian Privacy Principles set out in the Privacy Act 1988 (Cth).

Further Information

Further information about our Internet Banking Service is available at our branches, on our website **bankfirst.com.au** or by contacting us on **1300 654 822**. For further information on Internet Banking related Accounts and payment facilities, refer to our Product Terms and Conditions available at our branches, on our website **bankfirst.com.au** or by contacting us on **1300 654 822**.

Head Office
117 Camberwell Road
Hawthorn East VIC 3123
PO Box 338
Camberwell VIC 3124

bankfirst.com.au | 1300 654 822

Victoria Teachers Limited ABN 44 087 651 769
AFSL/Australian Credit Licence Number 240 960
MSID110 200819 - Effective from 20 August 2019