

CCF ONLINE ACCESS



New Authority OR Alteration to existing Date

Account Name (for Business account holders only)

Full Name D.O.B.

Address

Home no. Mobile no. Work no.

I/We have read and acknowledge the Terms and Conditions of CCF Online, outlined on page 3 of this document, and apply for access to my/our accounts through the CCF Online service. I/We authorise the following users to have access to my/our accounts as listed on page 2.

I/We understand that Full Access will enable the nominated personnel or person(s) to view account information and perform transactions on the nominated accounts including the transfer of funds to external Organisations and Individuals.

I/We acknowledge that anyone who has access to the Passwords may be able to transact on these accounts and it is the responsibility of the undersigned to protect the Passwords and not disclose them to anyone else.

I/We accept full responsibility on behalf of the nominated users for ensuring that payment details are correct, and acknowledge that CCF has no liability for any payment made in accordance with details provided.

I/We will inform CCF immediately there is any suspicion that the security of the Passwords has been breached.

I/We will advise the CCF immediately of any changes to the online authority.

I/We request CCF Online for all my accounts grouped under the above account number, except for the following accounts:

List all accounts types NOT to be linked to CCF Online:

Authorised Account Signatory

Date

Authorised Account Signatory

Date

**This authority must be signed in terms of the Authority to operate held by the CCF. This authority for linking accounts to CCF Online will be held with the normal authority to operation accounts. By signing this the authorised account signatory has read and understood all terms and conditions.*

0005013450/20231204

USERS AUTHORISED FOR 'FULL ACCESS' ON THE ABOVE ACCOUNT ARE: _____

Full Name	<input type="text"/>	D.O.B.	<input type="text"/>
Address	<input type="text"/>		
Home no.	<input type="text"/>	Mobile no.	<input type="text"/>
		Work no.	<input type="text"/>
Email	<input type="text"/>	Signature	<input type="text"/>

Full Name	<input type="text"/>	D.O.B.	<input type="text"/>
Address	<input type="text"/>		
Home no.	<input type="text"/>	Mobile no.	<input type="text"/>
		Work no.	<input type="text"/>
Email	<input type="text"/>	Signature	<input type="text"/>

Full Name	<input type="text"/>	D.O.B.	<input type="text"/>
Address	<input type="text"/>		
Home no.	<input type="text"/>	Mobile no.	<input type="text"/>
		Work no.	<input type="text"/>
Email	<input type="text"/>	Signature	<input type="text"/>

Method of operation for CCF Online: Sole Jointly

Note: Copy of Drivers Licence (front & back) for each person being given the authority to operate is to accompany this application, unless previous identified on the above account. Copy to be certified a true copy of the user's licence by the Authorised account signatory.

THE 'ENQUIRY ONLY' USERS WILL BE: (Choose only one type of access for each role) _____

Full Name	<input type="text"/>	D.O.B.	<input type="text"/>
Address	<input type="text"/>		
Home no.	<input type="text"/>	Mobile no.	<input type="text"/>
		Work no.	<input type="text"/>
Email	<input type="text"/>	Signature	<input type="text"/>

Full Name	<input type="text"/>	D.O.B.	<input type="text"/>
Address	<input type="text"/>		
Home no.	<input type="text"/>	Mobile no.	<input type="text"/>
		Work no.	<input type="text"/>
Email	<input type="text"/>	Signature	<input type="text"/>

Full Name	<input type="text"/>	D.O.B.	<input type="text"/>
Address	<input type="text"/>		
Home no.	<input type="text"/>	Mobile no.	<input type="text"/>
		Work no.	<input type="text"/>
Email	<input type="text"/>	Signature	<input type="text"/>

CCF USE ONLY

Date received Date processed Processed by

TERMS AND CONDITIONS

1. Keep accurate records of daily transactions completed on CCF Online and reconcile account details regularly.

- 1.1. CCF Online does not maintain a "mirror processing" backup system for transactions entered during the day. The transactions are backed up during the end of day processing which normally occurs at 4.30pm Monday to Friday. If for some unforeseen reason the CCF is required to restore account files back to the end of the previous days processing and re-enter the current days transactions, all CCF Online transactions will have to be re-entered by the client. This may prove to be difficult unless the client and user have a good system for recording daily transactions processed.
- 1.2. The client will not be advised immediately if account numbers are incorrect and they are fully responsible if they direct credit/debit the wrong account at another bank. Any fees associated with the incorrect debit or credit of an external account will be passed on.

2. Important issues the Client must be aware of when authorising access to CCF Online.

- 2.1. The Principal Account Holder authorises the CCF to allow access to each account to specific access levels for each user. Access to CCF Online may be terminated by the Principal Account Holder at any time by giving notice to the CCF in writing.
- 2.2. The Principal Account Holder authorises the Logon Name and Password used by the user(s) with the authority to operate, to be the authorised signatories on the nominated accounts through CCF Online.
- 2.3. The Principal Account Holder takes full responsibility for all value and non-value transactions through CCF Online that use the Principal Account Holder's or user(s)' correct Logon Name and Password.
- 2.4. CCF may terminate or suspend access to CCF Online by the Principal Account Holder or the user(s) for any reason. If account access is terminated or suspended you will be notified and provided reasons for termination or suspension and actions that may be taken to reinstate your account access.
- 2.5. The Client acknowledges and accepts that the CCF cannot verify by way of signature comparison whether CCF Online access was correct and accepts that the use of the correct Logon Name and Password is the equivalent of a signature.

3. Security

- 3.1. Browser based and uses the latest 128 bit encryption technology and verisign security which is the same high level of encryption technology as many of the leading Financial Institutions. The user can confirm their CCF Online session is encrypted by the appearance of a "lock" symbol at the foot of the browser.
- 3.2. User(s) are issued with a Logon Name and Password only after the Principal Account Holder's authorisation has been received. The first time a user logs on to CCF Online with a new or replacement Password they will be automatically prompted to change their Password.
- 3.3. As additional security user(s) have the option to change their Logon Name to their own preference.
- 3.4. User(s) are able to transfer funds within the Principal Account Holder's own accounts or to other clients' accounts with the CCF but are unable to transfer funds to external financial institutions or other CCF's unless authorised by the Principal Account Holder.
- 3.5. If a user suspects there has been or may be unauthorised access, the CCF can disable access immediately upon receipt of advice.
- 3.6. Transfer of funds to external financial institutions will be processed once daily at 2:30 p.m. on a banking day.
- 3.7. After 5 minutes an inactive web page will be automatically logged off by the system. A new internet session must be commenced if the host session is inactive for a further 2 minutes.
- 3.8. Access will be blocked if there are 3 successive unsuccessful login attempts during a 24 hour period (from Midnight daily). Access may only be restored through the CCF who will restore access after ascertaining identity of user.
- 3.9. There are two levels of authorised access available for each account for each user.
- 3.10. There is a record of all communication on CCF Online. All transactions processed through CCF Online are processed with normal "batch" transactions and will show on CCF hard copy reports.
- 3.11. Credit external Payments will be subject to a daily limit, which must be authorised by the Principal Account Holder.
- 3.12. Debit external accounts will be subject to a transactional limit authorised by the Principal Account Holder and accounts must be pre-nominated.

4. Principal Account Holder's Security Precautions

There are several key precautions that should be observed by Principal Account Holders and users when using CCF Online.

- 4.1. Password must be kept secret and secure.
- 4.2. Never leave a computer unattended while logged on to CCF Online.
- 4.3. Do not use date of birth, telephone number, address, name or names of friends, relatives or associates in a Password.
- 4.4. Change Password regularly, at least monthly is recommended.
- 4.5. Always exit CCF Online when finished by clicking on the log off button.
- 4.6. Use a reputable Internet provider.
- 4.7. Always use the latest available virus scanning software or virus signature file.
- 4.8. Keep complete and accurate records of daily transactions initiated through CCF Online.
- 4.9. The Principal Account Holder is to ensure the CCF has a current and accurate account operating authority.