



# Burnham on Crouch Town Council Internet Banking Policy

**Adopted 12<sup>th</sup> JUNE2023**

**Review date JUNE 2024**

## INTERNET BANKING AND ELECTRONIC PAYMENTS

Payment of invoices online saves time and money – no envelopes or stamps are required, and the authorisation can be done remotely at any time. The payment is received in the creditor's account within two working days; and the creditor does not have to take a cheque to their bank or risk cheques being lost in the post.

The controls and approvals, properly used, are as secure as the existing cheque system.

The Chief Officer and Office Clerk may 'view and submit' online **but must not authorise a payment**. Signatories may 'view and authorise' what the Chief Officer or Office Clerk has entered **but must not set up a beneficiary or a payment themselves**.

The Chief Officer will continue to provide Bank Statements and reconciliation with the Rialtas Business Solutions or Excel spreadsheet accounting package, to the Full Council at every meeting.

The Chief Officer will continue to make payments by cheque when and where necessary, following the existing controls and approvals, but will move to online payments when possible.

The Council will have a minimum of four Councillors as authorised signatories at any one time.

### Current position: April 2023

Burnham on Crouch Town Council has one account with Barclays Bank.

Burnham on Crouch Town Council has two accounts with Unity Trust Bank:

- a Current Account with a cheque facility and internet banking facilities for the day-to-day payment of invoices and receipt of any income; and
- a Reserve Account for any reserve funds that the Council might hold.

Four Councillors will be authorised signatories, including the Mayor.

## POLICY

1. Where internet banking arrangements are made with any bank, The Chief Officer and Office Clerk shall be appointed as the Administrators. The Chief Officer and Office Clerk will have 'view and submit only' authorisation. Transfers to and from accounts can only be authorised by the Mayor, Chief Officer, and Office Clerk, who will only be able to transfer funds between accounts held at the same bank.
2. The Bank Mandate approved by the Council shall identify four Councillors as signatories who will be authorised to 'view and approve only' transactions on those accounts. One of these signatories will be the Mayor.

3. Access to internet banking accounts will be directly to the bank's log-in page (which may be saved under "favourites") and not through a search engine or e-mail link. Remembered or saved password facilities must not be used on any computer used for Council banking work. Breach of this requirement will be treated as a very serious matter.
4. The Council, and those Signatories using computers for the Council's internet banking, shall ensure that anti-virus, anti-spyware and firewall software with automatic updates, together with a high level of security, is used.
5. No employee or Councillor shall disclose any PIN or password, relevant to the working of the Council or its bank accounts, to any person not authorised in writing by the Council.
6. New beneficiary details and changes to beneficiary details used for internet banking must be supported by hard copy or email notification, for checking and authorisation by two Signatories.
7. All transactions require two Signatories to authorise.
8. Payment for salaries, utility supplies (energy, telephone, and water) and any Non-Domestic Rates may be made by variable Direct Debit provided that the instructions are signed by two Signatories and any payments are reported to Council as made. The approval of the use of a variable Direct Debit shall be renewed by resolution of the Council at least every year.  
  
Any additional payments for overtime and mileage expenses can be made via online banking on an ad hoc basis and authorised by the required signatories.
9. Payment for items may be made by internet banking transfer, BACS or CHAPS provided that evidence (receipts and invoices) is retained showing which members approved the payment.
10. Standing Orders will not be used.

## PROCEDURE

### Procedure for **Setting up** Beneficiaries:

- a. The Chief Officer enters the details of the beneficiary online, via the internet banking URL. The Mayor and Office Clerk check these details, via the same URL.
- b. The Chief Officer emails a scanned copy of the BACS details of the beneficiary to the Signatories.
- c. Two Signatories check the details and authorise the beneficiary. **At no time should the Chief Officer or Office Clerk authorise the payment.**

### Procedure for **Changing** Beneficiary details

- a. The Chief Officer enters the amended details of the beneficiary online via the internet banking URL. The Office Clerk and Mayor check these details via the same URL.
- b. The Chief Officer emails a scanned copy of the new BACS details of the beneficiary to the Signatories.
- c. Two Signatories check the details and authorise the beneficiary. **At no time should the Chief Officer or Office Clerk authorise the beneficiary.**

### Procedure for **Paying** Beneficiaries:

- a. All invoices and requests for payment will be verified for accuracy by the Chief Officer/Office Clerk.
- b. The Chief Officer will list all payments required on the agenda for each meeting of the Full Council for approval. Invoices or other documentation will be initialled by the Mayor at the meeting.
- c. Wherever possible, payments will be made using online banking.
- d. Two authorised Signatories will confirm the payments online.
- e. Where payments are required in between meetings, the Chief Officer will email copies of the invoices requiring payment to the Signatories before setting up a beneficiary and/or placing a payment request online.

- f. **Signatories must not authorise a payment to themselves under any circumstances.**
- g. All requests will be emailed to all Signatories. To simplify the authorisation process two named Signatories will be the usual authorisers, with the others copied into the email.
- h. A new EU Payments Services Directive (PSD2) took effect in January 2018, bringing in new laws aimed at enhancing consumer rights and reducing online fraud. A key element of PSD2 is the introduction of additional security authentications for online transactions, known as strong customer authentication (SCA).
- i. After the changes were implemented in Autumn 2019, certain activity on Internet Banking now requires a second factor of authentication. In practice, this means the authoriser is asked to enter a code shown on the Internet Banking screen following receipt of an automated telephone call, to confirm they are the person making the request. The telephone message will confirm the details of the payment so they can be sure they are authorising the correct information and the call is genuine.
- j. There are additional actions within Internet Banking that will require SCA, these include:  
Accessing transactions and statements over 3 months old.  
Logging in every 3 months; and  
Making changes to beneficiaries' payment details e.g. changing the destination account number or sort code.
- k. Only the individual submitting the payment will be called and they will be contacted on the number/s they have registered with the bank. They will be informed at the point of making the payment that additional security is required before the payment can be made, therefore they will need to have access to their telephone before starting their online banking activities.

Date of policy: 12<sup>th</sup> June 2023

Approving committee: Full Council

Date of committee meeting: 13<sup>th</sup> April 2023

Policy version reference: Version 3.1

Supersedes: Version adopted September 2019

Policy effective from: 12<sup>th</sup> June 2023

Date for next review: 2024