SCOTTON PARISH COUNCIL

INTERNET / TELEPHONE BANKING AND DEBIT CARD POLICY

UP DATED OCTOBER 2024

"The Legislative Reform (Payments by Parish Council, Community Councils and Charter Trustees) Order 2014 came into effect on 12th March 2014." It repealed the statutory requirement for two elected members to sign cheques and other orders for payments.

This enables Scotton Parish Council ("The Council") to consolidate its money controls and introduce on-line banking to take advantage of modern technology.

Introduction

The Council:

- maintains robust controls on payments as part of its integrated financial control system and introduces this policy as an addendum to its Financial Regulations.
- approved payment by on-line banking, telephone or debit card at its meeting on 5th May 2022.
- has 3 cheque signatories: Cllr R.Walker.Cllr M.Johnsonand and Cllr Y.Huddleston
- has 3 signatories for the on-line account: Cllr. R Walker,Cllr M.Johnson and Cllr Y.Huddleston
- has 1 named debit cards; Cllr.R. Walker

This policy forms an addendum to the Council's Financial Regulations and is to be read in conjunction with adopted Financial Regulations and Standing Orders.

The Parish Council has two accounts with TSB Bank:

- Current account with cheque, debit card and internet and telephone banking facilities for the day-to-day payment of invoices and receipt of any income.
- Savings account for holding

Online transactions and telephone banking payments must be approved at a full Council meeting in advance.

Procedure for cheque payments

This procedure is unchanged; cheques (and counterfoils) will be signed by two Councillor signatories.

Procedure for on-line and telephone banking

- Where internet banking arrangements are made with any bank, the Chairman shall be appointed as the Administrator.
- Only the Chairman will be authorised to make pre-approved payments or intra-net transfers between accounts; this would be the current account and the reserves.
- Access to the internet banking account will be directly to the bank's log-in page (which may be saved under "favourites") and NOT through a search engine or email link.
- Remembered or saved password facilities must not be used on any publicly accessed computer, on any other computer or devices with internet capacity that could be accessed by unauthorised persons.
- Internet signatories will not use remembered or saved password facilities when using private laptops.
- Breach of this requirement will be treated as a profoundly serious matter as it could nullify and void the Council's fidelity insurance if the Council were to be hacked.
- 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.
- If an iPhone, android, or smart phone are used by a signatory; the phone must have anti-virus, anti-spyware, and firewall software with automatic updates, together with a high level of security. If the phone is lost and is known to contain sensitive financial information, the Council must be advised as soon as possible, if it is stolen - its loss must be reported to the Council and the police. The named signatory will be temporarily unable to approve payments until a substitute phone is made safe or the lost phone is recovered, to limit any possible misuse or fraud.
- 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 or a duly delegated committee.

- All online, telephone and debit transactions shall continue to require prior approval by the Council, unless delegated authority or prior approval has been approved by the Council.
- Standing Orders and Direct debits are not to be used without resolution of the Council.

Procedure

Wherever possible, Council payments will be made using on-line or telephone banking.

The following principles and procedures apply to the operation of the on-line account with particular attention to the raising of payment requests and their authorisation. The actual process will additionally be subject to the rules and security authorisation processes of the enabling bank.

A schedule of all payments to be made shall be prepared by the Clerk/RFO and presented to the next meeting of the Council for approval.

Two non-signatory Councillors will check and sign the invoices or any other supporting paperwork.

Where payments of pre-approved Council spend are required between meetings, the Chairman will email copies of the invoices for payment to authorised signatories (and a non-Councillor signatory for additional scrutiny), requesting their email authority to proceed. This will be reported at the next full Council meeting.

Signatories may not authorise a payment to themselves.

If the Chairman, for reasons due to illness, incapacity or banking access difficulties is unable to carry out online or telephone payments, the Council may, by resolution of Council give approval for another internet signatory to make the payment. The Chairman will be kept informed of any payments made in this way.

.

DEBIT CARDS

In view of the increase of internet purchasing due to the potential saving that online purchasing may offer and the requirements of maintaining operations. The Council may authorise the issue of debit cards to named persons for business use only.

The issue of a Council debit card to the Clerk or any Council member must be authorised by the Parish Council and be issued to a named person for the sole use of Council business, no other individual may use the debit card.

Each named person issued with a debit card is solely responsible for its safe keeping and for ensuring that the card is not used by others. PIN numbers will be held securely by the clerk and not divulged to any named Councillor. The CSC/CVN number must always be kept confidential and not disclosed to any other person.

Lost or stolen cards must be reported to the issuing bank immediately upon discovery that the card is missing. With no exceptions the Chairman must also be informed immediately who will inform Council.

In the event of any named debit card holder, Councillor leaving the Council, the following must be done:

a) If a Councillor is leaving the Council, it who will destroy it and notify the bank.

Usage detailed

Cash withdrawals are not permitted.

The card shall not be used for any non-Council business transactions nor for any personal purchases.

Payments by a named debit card may only be made when it is not possible or practical to pay by cheque or bank transfer or where suppliers are unable to offer a credit account and must be used for authorised costs as indicated for other forms of payment.

Routine and minor transactions will have assumed approval with post event transaction reporting to the Council. An individual minor transaction is that below £50. In any period of a calendar month, the aggregate expenditure shall not exceed £100.

Each transaction is limited to £500 at any time in accordance with the Council's Financial Regulations.

Significant expenditure items of £500+ will require pre-expenditure approval by the Council.

There will be an annual review of debit card and on-line transactions to gauge accuracy, financial savings, ease of use and to check authorised signatories are up to date with any banking procedures or financial legislative changes and still wish to remain signatories. This will be confirmed at the Annual Meeting of the Council each year.

Reconciliation and inspection

Every debit card transaction must be entered on the cashbook account spreadsheet and spend detailed in the regular finance report

Receipts and invoices for all purchases must be submitted to, and checked by, the Council for signing off by two non-signatory Councillors.
All card payments will be included on the payments listing for presentation to Council for noting and for public scrutiny.
Transactions will be reconciled monthly with bank statements. In the event of any discrepancy two non-Councillor signatories will initiate an investigation.

The cardholder is responsible for obtaining and submitting receipts and invoices for all transactions. Failure to produce transaction receipts and invoices may result in the cardholder being held liable for the sum of the said transactions.

Fraudulent or Misuse of a Debit Card

If the cardholder misuses the debit card or fraudulently uses the card, this may result in disciplinary action being taken against the cardholder. The card holder must return the card to the Chairman whereupon it will be destroyed, and the bank notified.

Audit

- The Chairman is otherwise unable, any one of the other internet signatories will provide a copy of the bank statements (including the reserve account) at each Council meeting so all banking activity may be evidenced and minuted. If bank statements are unavailable, the Chairman or other Councillor will explain the reason, which will be minuted.
- The Chairman will retain copies of transaction requests and email authorisations in the annual finance file, for presentation to the Internal Auditor and any other official scrutiny.

Insurance

Any financial losses due to fraud or similar would fall under the Council's Fidelity Guarantee insurance, currently provided by Parish Protect Suffolk. The Council must ensure compliance of the Policy wording in Section Two, so as not to risk any security breaches. Security breaches, found to be the fault or responsibility of the Council would void the Council's insurance policy.