St Luke's NS 13648D

Electronic Banking Policy

Introduction:

St. Luke's NS uses electronic banking to keep up to date on its bank account(s) activity by viewing balances and accessing transaction history online including current account(s), merchant account(s) and credit card(s).

The online banking system also enables St. Luke's NS to import and export data to and from accountancy systems.

Online Banking would allow transactions to be uploaded to an Accounting System. However the Accounts System adopted and maintained is the FSSU Excel template and all transactions are recorded here. These are independently verified and reviewed annually by the BOM Independent Accountant.

Purpose of the Policy:

The purpose of this policy is to regulate the use of Electronic Banking within the school and forms part of the school's internal control procedures in relation to the following:

- Bank Accounts to be accessed using Electronic Banking
- Names of authorised users.
- Users access to functions of the system
- Authorisation of payments
- The inclusion of new bank accounts on the system
- Thresholds regarding transaction values
- Security controls regarding access to the system and passwords

Scope:

This policy relates directly to St. Luke's Electronic Banking.

General Principles:

1. The Board of Management of St. Luke's NS must approve the use of Electronic Banking within the school.
2. This must be noted in the minutes of a BOM meeting.
3. The Board must review and approve (and update when necessary) this policy on an annual basis.

Bank Accounts and Credit Cards:

St. Luke's NS currently do our banking with AIB and we are set up to take payments for activities through Aladdin using a merchant services account provided by Elavon (this is linked back to the main AIB bank account). We also have a credit card provided by AIB.

All bank accounts and credit card accounts with AIB can be accessed via Electronic Banking through:
https://aib.ie/business/business-login/business-banking-online

Athbhreithnithe 02/02/2023

St Luke's NS 13648D

The online banking system requires approval of payments by two users using individual digi passes.

Lodgements are made direct by Government Agencies or by Treasurer using the BOM Banking Card

Elavon account can be accessed through:
https://www.elavonconnect.com/ui/#/eu/en_GB/welcome

Elavon security manager can be accessed through:
https://elavonsecuritymanager.com/safemaker/login/portal

Authorised Users/Access:

The three current authorised users are as follows:

1. BOM Treasurer (Administrator) - Input Payments and Authorise Payments, view systems, print documents, add/delete accounts (with board approval minuted at a BOM meeting), set up standing orders/direct debits (with board approval and minuted at BOM meeting)
2. School Principal - Authorise Payments, view systems, annual PCI compliance (Elavon).
3. BOM Chairperson (Administrator) - Authorise Payments, view systems.

Segregation of Duties:

All payments require two approvals. One user (BOM Treasurer) will input a payment on the system and approve. A different user (the Principal/Chairperson), must do the final authorisation of the payment.

It is the responsibility of those authorised individuals to ensure adequate checks have been made and payments are transferred to the correct bank accounts, in line with the Electronic Banking Policy.

Payments can be made to external third parties and inter account transfers.

Where possible there is a segregation of duties of persons Authorising and Recording transactions. Each transaction is vouched by third party evidence (Purchase Invoice, Receipt). Such evidence is maintained under Statute of Limitation rules for review by Independent Accountant and State Auditor.

Thresholds for Euro Value of Transactions:

Thresholds for euro value of transactions per day/week/month/per authorised user (BOM Treasurer) are approved by the board and set at a realistic level having regard to the average recurring payroll costs etc.

Payment thresholds are set at €10,000 per transaction per day. These are flexible and can be changed by approval of the two users.

Security Controls:

All passwords/usernames/codes must be stored securely and separately. New passwords/usernames/codes will be generated with the change of any personnel and old login details etc should be disregarded and destroyed.

Athbhreithnithe 02/02/2023

There should be **no** sharing of login details or passwords.

It is the responsibility of each user to store login details and passwords securely.

It is the responsibility of each user to disregard and destroy any personal and old login details and passwords.

St. Luke's NS allows the use of a Password manager, but this would be an expense borne by the user.

Changes to Payee Details:

Any changes to payee details must be confirmed by phone call to a known contact at the supplier, or in person, and approved by the authorisers (listed above) **before** any changes are made.

Vigilance around Requests to Change Supplier Bank Information:

Vigilance around emails in relation to changes in supplier details (especially bank information) should be high. Email contact around this area should be limited as this is where fraudulent activity may originate.

Ratification of Policy, Review and Monitoring

This policy will be reviewed by the Board of Management annually in the first term.

This policy was adopted by the Board of Management in the 2022/23 school year.

Signed: _____
Chairperson of Board of Management

Date: 5/11/24

Signed: _____
Principal

Date: 5/11/24

Next Review Date: Term 1 2025/26 school year.