FSSU
Financial Support Services Unit

Further Guidance on Electronic Banking

Introduction

Electronic banking allows the school to keep up to date on its bank account(s) activity by viewing balances and accessing transaction history online including deposit accounts and credit cards. The online banking system has the added benefit of enabling schools to export and import data to and from their accountancy systems.

Authorisation

The decision to implement an Electronic Banking System must be made by the board of management. This decision must be approved and noted in the boards' minutes. Once the decision to implement an Electronic Banking System has been taken, the board must ensure that an Electronic Banking policy is implemented as part of school the schools' internal control procedures.

Internal control procedures

This document must clearly outline the use of Electronic Banking within the, with clear instructions in relation to the following:

1. Bank accounts to be accessed on Electronic Banking.
2. Names of authorised users.
3. Users access to functions of the system by individual users e.g. view only, print only, authorise payments, add new accounts, delete accounts, set up standing orders / direct debits etc.
4. All payments must ultimately be authorised by the Principal and one other nominated by the board within the existing current account mandate in line with the controls in place for making payments by cheque.
5. The inclusion of new bank accounts onto the system and the deletion of old accounts from the system must also be approved by the board in a similar manner.
6. Thresholds regarding Euro value of transactions per day / week / month / per authorised user, should be approved by the board and set at a realistic level having regard to the average recurring payroll costs.
7. Security controls regarding access to the system and passwords must be set out.

Security

The Electronic Banking policy should be reviewed and, where appropriate, updated at least once a year. The results of this review should be approved and noted in the minutes of the board.

- All passwords / user names / codes must not be stored within the office environment.

- Passwords / user names / codes should be confidential; therefore they must never be shared between individual users. They should be unique and individual to named authorised users of the Electronic Banking System
- Any separate handheld electronic devices that form part of the banking system (i.e. merchant bank terminals) should be securely stored under lock and key.

Segregation of duties

It is vital to ensure the segregation of duties when using an Electronic Banking System.

The Electronic Banking policy should detail the users responsible for different elements of the functions used on the system.

For example, one user may input a payment on the system and a different user/s may authorise the payment. Before payments are processed, 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.

In line with good financial practice, the person preparing the payment should not be one of the approvers on the payment.

Bank feeds and Bank Reconciliations

Bank account reconciliations can be assisted by availing of bank feeds. Bank feeds allow the school to link its online bank account (s) directly to the school's internal accounting system, so your banking transactions are automatically imported into your accounts. This reduces administration time and streamlines the bank reconciliations.