



Learning Through Play!

Scottish Pre-school Play Association

Internet Banking Guidance

There can be advantages to internet banking for a pre-school group. Treasurers can access the group's business account information without making a trip to the bank. Statements can be downloaded, balances can be checked and bills paid online, funds can be transferred from one account to another, even when the bank is closed, which saves both time and money.

Where groups opt to bank online, they should be aware of internet banking security and set up procedures which protect their account/s and minimise the risk of identity theft which is a real and growing problem. Groups need to be highly protective of their account information and ensure that personal information relevant to the group's account is never given out over the internet unless assured that the site is secure. It is good practice to routinely check your computer for spy ware and viruses, protecting your identity this way as well.

Before setting up internet banking the following points should be considered:

Setting up the account

The group's management committee should discuss whether to use internet banking at a committee meeting. If it is decided to proceed then procedures should be discussed, written and agreed to ensure that everyone is clear and aware of how the internet banking facility will be operated.

Procedures could include:

- Specifying who can use internet banking on behalf of the group, for example, the treasurer plus one other named person
- Specifying what financial transactions can be made using internet banking, for example, paying wages, making transfers from one account to another, payment of bills.

Only the individuals with agreed authorisation to manage the account should be aware of the account passwords and/or ID information. The account passwords and/or ID information must be kept securely.

Approval of Transactions

The person managing the internet banking system should **not** be able to approve the payments or transfer of funds without appropriate authorisation. All transactions must only be made with approval from the committee.

- Full approval from the committee at a committee meeting is required for larger items, for example invoices in excess of £40.
- Email authorisation from two office bearers on the committee not including the person managing the internet account for smaller items, for example invoices less than £40.

Monitoring the account

The passwords and/or ID information must not be changed without the authorisation of the committee at a management committee meeting. The password and/or ID information should always be changed when those managing an account change.

Store your access information in a secure place. A record of the passwords and/or ID information should be kept in a sealed envelope, marked confidential and stored securely.

Two people who are office bearers preferably the treasurer and chairperson should each receive a copy of the monthly bank statement posted to them directly from the bank. The treasurer should prepare a monthly bank reconciliation statement which should be presented and discussed at committee meetings. Accounts must be seen by the committee at each committee meeting. These should be transparent and easy for all to understand and signed off by the chairperson. Printouts should be taken of all payments, receipts and transfers and made available at each committee meeting.

To ensure good practice the agreed procedures should be reviewed annually by the committee.