Internal financial controls

(Including the additional controls needed to use on-line banking)

Guidance for keeping all WI accounts:

- All incoming monies **must** be banked regularly – and as quickly as possible after each meeting
- All incoming money **must** be banked gross - no amount held back for "feeding" petty cash or for paying expenses.
- All cash and cheques received and payments made are recorded in the account book including details of cheque numbers or reference of an on-line payment.
- Pay-in slips to agree with the amount banked and dates on bank statements
- Payments should only be made against **original** invoices. If an invoice is not available a docket should be signed to confirm receipt of payment.
- Two out of three signatories on cheques. Cheques made payable to a nominated signatory **must not** be signed by that person.
- Blank cheques **must never** be signed in advance - breach of financial control.
- WI cheque books should be kept in a secure place with limited access.
- The treasurer should be given the opportunity to make reports to the committee so that they are aware of the financial position of the WI
- The President should sign off regular bank reconciliations.
- A budget should be prepared by the treasurer and agreed by the committee at the start of each financial year.

Guidance for Electronic Banking

Additional safeguards needed for using electronic banking and computerised accounts:

- Transfers or other direct payments into the bank are identified and verified against supporting paperwork. These checks should be made by someone other than the person concerned with the original recording of the transactions.
- It is extremely important to have a reference system for identifying members paying subscriptions by BACS. There may be a number of members with the same surname.
- Electronic payments must be properly authorised by 2 members of the committee (some banks offer addition checks which can be used but nay be charged for).

Credit and charge cards

Many retailers no longer accept cheques leading to an increase in the use of card transactions.

Credit card payments are invoiced monthly and there is some ability to intervene in the case of misuse, but controls still need to be in place over their use. Used properly these methods of payment are generally considered to be safe, but certain controls need to be put in place, including setting a clear policy for the use of payments cards, the criteria for their issue, spending limits and their security;

- Keep the credit limit on the credit card below the level of the cash assets held by the WI.
- Set an upper limit on the amount allowed per transaction

- Place restrictions on the types of retailers where the cards may be used, eg blocking their use in betting shops and on certain websites;
- The members must pass the policy for the use of payment cards and a copy be kept, in writing, in the minute book
- Ensure payments cards are cancelled and destroyed when the signatory leaves the committee
- Ensure that card expenditure is supported by a docket and/or invoice and recorded and analysed in accounting records
- Copies of all credit or charge card statements should be examined by more than one member of the committee. The statements are used to record and analyse transactions in the accounting records and are matched with supporting dockets and invoices.

On-line Banking

Electronic banking is increasingly used by WIs as a convenient way to manage their transactions. Where electronic banking is used, the same level of internal financial controls should be in place as for more traditional forms of banking:

- It is even more important that more than one member of the committee authorises payments and checks that payments, goods and services have been received
- E-safety protocol should be considered by the committee and a policy put in place.
- Electronic accounts and records should be regularly backed up and a copy of all accounts kept by someone other than the treasurer.
- Check that the electronic banking URL starts with HTTPS (S for security)
- After each electronic banking transaction a print out should be made showing details of the transaction and stored as part of the records
- Print outs of bank statements can be downloaded but WIs should continue to receive paper copies
- PCs must be kept up to date with anti-virus, spyware and firewall software.
- Keep all the password(s) and PIN(s) secret. (It is important that more than one member of the committee has full access to the electronic accounts or knows how to access the records kept on a computer – have a dedicated ‘WI’ memory stick to back up to)
- Change passwords when treasurers change.
- Be alert to Phising attacks. Committee members should not respond to emails or telephone calls asking them to provide personal security details.

Debit Cards - *Beware*

Debit cards charge bank accounts directly and payments therefore have an immediate impact on bank balances; their misuse or loss can be extremely serious for the WI.