MC/10/29

Guidance on Internet Banking

Basic Information

Contact Name and Details	Nick Moore, Head of Support Services (MCH ext 5159)
Status of Paper	Final
Action Required	Information
Draft Resolution	
Alternative Options to Consider, if Any	

Summary of Content

Subject and Aims	This paper seeks to provide guidance on internet banking to Districts as recommended by the 2009 Methodist Conference following a report entitled "The use of Internet Banking for the Management of Church Accounts".
Main Points	• What is meant by 'Internet Banking'. • Guidance from the Charity Commission on whether internet banking should be adopted. • Steps to take to ensure that there is a clear segregation of duties. • The advantages and disadvantages to using internet banking. • Advice on computer security.
Background Context and Relevant Documents (with function)	• 2009 Methodist Conference Agenda – Resolution 44/3 • Standing Order 012 (1)
Consultations	Rodney Betts, Southampton District Treasurer Andrew Gibbs, Connexional Treasurer Ronald Calver, Connexional Treasurer

Summary of Impact

Standing Orders	
Faith and Order	
Financial	
Personnel	
Legal	
Wider Connexional	
External (e.g. ecumenical)	
Risk	

Guidance on Internet Banking

What is Internet Banking?

Internet banking allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society. It is a system of banking in which customers can view their account details, pay bills, receive payments and transfer money by means of the Internet. You may also be able amend or cancel payments by regular standing order (dependant on which bank you use).

Is Internet Banking Appropriate for your Church situation?

The Charity Commission in their guidance on electronic banking have said that a charity is justified in using internet banking if:

- "They can identify overall advantages for the charity in doing so;
- They put in place adequate financial controls; and
- They have, or can acquire, the necessary legal power."

They go on to say:
"It is important that any decision to adopt electronic banking be made with the benefits and advantages to the charity in mind, It is not right to move to electronic banking just because it seems fashionable or because the charity's bank want it to change (the motive for this might be to help the bank reduce its own costs, rather than provide a better service for the charity)."

It is essential that if you decide to use internet banking that you have the same level of financial controls that you would already have with your existing banking system.

The recently amended SO - 012(1) gives holders of Methodist accounts the legal power to conduct banking via the internet and states:
"Methodist money shall not be held in private accounts but in official bank accounts requiring *[. . .] the* signatures *of, or electronic authorisation by, two persons* for withdrawals."

It is therefore crucial that there should continue to be a clear segregation of duties, to make sure that no one individual is able to control your resources.
A number of High Street financial institutions offer internet banking that allows this requirement to be met through a dual authorisation system. Some banks may charge for this facility however the following banks do not:

- CAF Bank
- Triodos Bank - although there is a one off £10 fee for providing a Digipass to each authorised user.
- Unity Trust Bank

The best procedure to adopt to ensure dual authorisation is as follows:

Step 1: Someone, not necessarily a signatory, prepares the payment request electronically. A copy of the internet transaction could be printed off for your records.

Step 2: A signatory of the account approves the payment - this may also be the person that prepares it.

Step 3: A second signatory releases the payment providing that they are happy with it. If they are not they should seek documentary evidence.

Once the payment has been checked and released a copy of the internet transaction could also be printed off at this stage to complete your records of the whole transaction.

The Advantages and Disadvantages of Internet Banking

There are a number of advantages and disadvantages to using internet banking and it is important that you take these into account before deciding whether to use it for your Methodist account.

Advantages:

- It could potentially reduce item charges and postage due to the reduction in the number of cheques used.
- Banking can be done out of working hours in the evenings and weekends. Transactions can be carried out 24 hours a day, 7 days a week and are not restricted by bank opening times. This may be the main advantage for volunteer treasurers.
- The two signatories can initiate and authorise payments as required without needing to meet physically – useful within large circuits and districts.
- You can instantly see what is happening with your money and do not have to wait for statements.

Disadvantages:

- Computer equipment and internet access is necessary and this could mean additional costs if they are not already available.
- Some banking institutions may charge for the services of the bank.
- There are a limited number of banking institutions offering this facility at this time.
- Your existing bank may not offer the necessary dual authorisation facility necessitating a change in provider
- Internet banking requires a level of personal computer skills and some training may be necessary.
- The bank may require the signing of an indemnity that says the Church/District agrees to cover the bank for all costs and losses it sustains arising from the use of internet banking.

Computer Security

To ensure that the church's accounts are secure from external parties or any internal misuse it is necessary to look at your overall computer security. Here are some particular areas of concern that you should consider:

Pin Protection:

- It is essential that you protect your PIN. Memorise your PIN and destroy any written notification you have received. Never write down/record your PIN down, or store it on your mobile phone. Never share your PIN with anyone and do not allow anyone else to use your PIN.

- If you have difficulties remembering it change to something more memorable but ensure that it is not obvious or too simple - do not use dates of birth, consecutive digits etc.
- If you think someone has seen or learnt your PIN, change it immediately. Always check your statements regularly to keep track of your transactions and if you see an unfamiliar transaction contact your banking institution immediately.

Password Protection:
- The longer your password is the better. Do not just use letters, but also use numbers or punctuation.
- Keep your password anonymous and avoid using personal information such as birth dates, names or any other personal information so no one can guess it.
- Passwords should be changed periodically - maybe every 6 months.

Virus Protection:
- Use anti-virus and anti-spyware programs. Update them regularly to ensure they are at their highest level.

Firewall:
- Log onto the internet through a firewall, a program or technical equipment minimising the risk or access to your computer via the internet. This will enable you to deal with queries permitted by you whilst filtering out any potentially dangerous data.

Unknown Files and Emails:
- Only use well known and trustworthy internet websites.
- Do not download unknown files from the internet (especially those with an EXE extension).
- Do not open emails from unknown senders or messages from suspicious names or containing suspicious contents. Delete them without opening them.
- Never respond to an email requesting your password, PIN or any personal information.

Enhance your security:
- To ensure that you can detect unauthorised transactions you may wish to adopt a SMS/email message service which will let you know when transactions have been made on your account. Many banks offer this service.