

Financial Guideline 2018/2019 - 13

Community & Comprehensive and Voluntary Secondary schools

Electronic Banking

Introduction

Electronic banking, also known as internet banking, e-banking or virtual banking, is an electronic payment system that enables schools to conduct a range of financial transactions through their banks website.

There are advantages to using e-banking both for banks and schools such as permanent access to the bank, lower transaction costs/general cost reductions, access anywhere, less time consuming, very safe and secure method, transfer money immediately and accurately and security of the account.

A. Electronic Banking set-up

1. Approval must first be obtained from the board of management for the use of electronic banking by the school. This approval should be included and approved in the minutes of the board meeting
2. Contact your local Bank to organize electronic banking for the school
3. The electronic banking software will need to be loaded onto the computers of the approved Bank Signatory per the Bank Mandate and on the computer of accounts personnel
4. An electronic payment is subject to the same rules as a cheque payment and therefore must be approved by the Principal and another signatory as per the Bank Mandate that has been approved by the board
5. In line with good financial practice, the person preparing the payment should not be one of the approvers on the payment
6. The accounts personnel can access the electronic banking system to set up and prepare payments and download bank statements
7. Access to approval of electronic payments must be password protected. It is not permissible for a Bank Signatory to tell anyone else this password

8. Additions and amendments to suppliers/employees being paid by on the electronic banking system must be approved by the Principal and another Bank Signatory
9. It is the responsibility of the Principal to ensure that the bank is aware of these controls and that the electronic banking system implemented complies fully with these controls

B. Access your accounts from a secure location

It's always best practice to connect to the school bank account using computers and networks you know and trust. Be cautious if you use open Wi-Fi such as those provided in hotel lobbies, shops etc. Try to avoid using Internet cafes or a computer that is not your own.

C. Monitor your accounts regularly

It should go without saying that monitoring your bank statement when received is good practice as any unauthorised transactions will be identified on a timely basis. Take advantage of the feature in online banking and check the account on a regular basis. Look at every transaction and if you see any anomalies, contact your bank immediately.

D. Always log out when you are finished

It is good practice to always log out of your online banking session when finished. This will lessen the chances of falling prey to session hijacking and cross-site scripting exploits.

E. Do not share passwords for online payment systems

When passwords are shared between staff, the anti-fraud control and segregation of duties become void and the process is left open to fraudulent practice. Staff should always be educated about password abuse and associated risks and passwords should have regular, system generated changes.

F. Upgrade computer security

As the threat of cyber-crime continues to increase globally, schools need to update anti-virus software and make sure adequate school firewalls are in place. This will defend against malware attacks and deter intruders from accessing your computers. At a time when computers are easily hacked and remotely controlled by criminals, effective anti-virus software will detect and quarantine dangerous files and programs.

Further information or clarification on any of the issues raised in this Guideline can be obtained from the FSSU.

Tel: 01-269 0677

info@fssu.ie

22nd November 2018

Treoirlíne Airgeadais 2018/2019 - 13

Pobalscoileanna, Scoileanna Cuimsitheacha agus Meánscoileanna Deonacha

Ríomhbhaincéireacht

Réamhrá

Is ionann ríomhbhaincéireacht, ar a dtugtar baincéireacht idirlín, r-bhaincéireacht nó baincéireacht fhíorúil chomh maith, agus córas ríomhíocaíochta lena gcumasaítear do scoileanna raon idirbheart airgeadais a dhéanamh trí láithreán gréasáin a mbainc.

Baineann roinnt buntáistí le ríomhbhaincéireacht do bhainc agus do scoileanna araon, amhail rochtain ar an mbanc i gcónaí, costais idirbheart níos ísle/costais ghinearálta laghdaithe, rochtain ó áit ar bith, níos lú ama i gceist, aistriú láithreach agus cruinn airgid agus slándáil an chuntais.

A. Ríomhbhaincéireacht a chur ar bun

1. Ní mór cead a fháil ón mbord bainistíochta ar dtús chun an ríomhbhaincéireacht a úsáid sa scoil. Ba cheart an cead sin a chuimsiú agus a fhaomhadh i miontuairiscí chruinniú an bhoird
2. Déan teagmháil le do Bhanc áitiúil chun ríomhbhaincéireacht a eagrú don scoil
3. Ní mór na bogearraí ríomhbhaincéireachta a lódáil ar ríomhairí an tSínitheora Bhainc fhaofa de réir an tSainordaithe Bhainc agus ar ríomhaire phearsanra na gcuntas
4. Tá ríomhíocaíocht faoi réir na rialacha céanna is atá íocaíocht le seic agus dá bhrí sin ní mór don Phríomhoide agus do shínitheoir eile í a fhaomhadh de réir an tSainordaithe Bhainc atá faofa ag an mbord
5. I gcomhréir le dea-chleachtas airgeadais, níor cheart don duine a réitíonn an íocaíocht a bheith ar dhuine dóibh siúd a dhéanann an íocaíocht a fhaomhadh.

6. Is féidir le pearsanra na gcuntas rochtain a fháil ar an gcóras ríomhbhaincéireachta chun íocaíochtaí a shocrú agus a ullmhú agus chun ráitis bhainc a íoslódáil
7. Ba cheart rochtain ar fhaomhadh ríomhíocaíochtaí a chosaint le pasfhocal. Ní cheadaítear do Shínitheoir Bainc an pasfhocal sin a insint d'aon duine eile
8. Má dhéantar na soláthraithe/fostaithe atá á n-íoc ar an gcóras ríomhbhaincéireachta a leasú nó daoine breise a chur leis, ní mór don Phríomhoide agus don Sínitheoir Bainc eile é sin a fhaomhadh
9. Is faoin bPríomhoide atá sé a chinntiú go bhfuil an banc ar an eolas i dtaobh na rialuithe sin agus go bhfuil an córas ríomhbhaincéireachta a chuirtear i bhfeidhm i gcomhréir leis na rialuithe sin ina n-iomláine

B Faigh rochtain ar do chuntais ó áit shlán

Tá sé ina dhea-chleachtas i gcónaí nascadh le cuntas bainc na scoile trí ríomhairí agus líonraí a bhfuil thaithí agat orthu agus a bhfuil iontaoibh agat astu. Bí cúramach má úsáideann tú Wi-Fi oscailte, amhail na cinn a bhíonn ar fáil i bhforhallaí óstán, siopaí srl. Ná bain úsáid as caiféanna idirlín ná as ríomhaire nach leat féin é.

C. Déan monatóireacht rialta ar do chuntais

Ní gá a rá go bhfuil sé ina dhea-chleachtas monatóireacht a dhéanamh ar do ráiteas bainc nuair a fhaigheann tú é, mar ar an gcaoi sin d'aithneofa aon idirbhearta neamhúdaraite go pras. Bain leas as an ngné sa bhaincéireacht ar líne agus déan an cuntas a sheiceáil go rialta. Féach ar gach idirbheart agus má aithníonn tú aon aimhrialtachtaí téigh i dteagmháil le do bhanc láithreach.

D. Logáil amach nuair atá tú críochnaithe leis i gcónaí

Is dea-chleachtas é logáil amach as do sheisiún i mbaincéireacht ar líne nuair atá tú críochnaithe leis. Ar an gcaoi sin, ní bheidh an deis chéanna ag daoine fuadach seisiúin ná scriptiú cros-suímh a dhéanamh.

E. Ná déan pasfhocail le haghaidh córais íocaíochta ar líne a chomhroinnt

Nuair a dhéanann baill foirne pasfhocail a chomhroinnt, cuirtear an rialú frithchalaíoch agus leithscaradh dualgas ar neamhní agus bíonn an próiseas i mbaol ó chleachtas calaíoch. Ba cheart baill foirne a chur ar an eolas i gcónaí faoi mhí-úsáid pasfhocail agus na rioscaí lena mbaineann, agus ba cheart athruithe rialta, arna nginiúint ag an gcóras a dhéanamh orthu.

F. Déan slándáil ríomhaireachta a uasghrádú

Toisc go bhfuil baol na cibearchoireachta ag méadú ar fud an domhain, ní mór do scoileanna nuashonrú a dhéanamh ar a mbogearraí frithvíreas agus a áirithiú go bhfuil ballaí dóiteáin iomchuí ar bun acu. Ar an gcaoi sin, cosnófar iad i gcoinne ionsaithe ó bhogearraí mailíseacha agus déanfar ionróirí a dhíspreagadh ó rochtain a fháil ar a gcuid ríomhairí. I dtráth inar féidir le coirpigh ríomhairí a haiceáil agus a cianrialú go héasca, déanfar comhaid agus cláir dhainséaracha a bhrath agus a chur ar coraintín le bogearraí frithvíreas éifeachtacha.

Is féidir tuilleadh eolais nó soiléiriú a fháil ar aon cheann de na saincheisteanna sa Treoirlíne seo ach dul i dteagmháil le FSSU.

Teil: 01-269 0677

info@fssu.ie

An 22 Samhain 2018