FSSU
Financial Support Services Unit

Emmet House, Milltown, Dublin 14
Tel: 01 2690677 Email: info@fssu.ie

Financial Guideline 2017/2018 - 17

Community & Comprehensive and Voluntary Secondary Schools

IT Infrastructure Checklist

Introduction:

Following a number of security issues relating to IT arising in schools, we have compiled the following checklist to identify a minimum configuration which should be in place in order to operate an up-to-date, secure and reliable IT infrastructure for secondary schools.

The aim of the checklist is to help you identify any issues which need to be addressed and provide you with best practice information. Importantly, it is not a substitute for a detailed infrastructure assessment which should be performed by your IT service provider.

If you are having difficulty answering any of the questions your IT service provider should be able to assist.

1. Policies

	Usage policy	
1.	Does your school have computer usage guidelines in place and are they up-to-date? Typical policies would include: • Acceptable Use Policy • Internet Access Policy • Email and Communications Policy • Network Security Policy • Remote Access Policy • BYOD Policy • Encryption Policy • Privacy Policy	Yes /No
2.	Have the guidelines been brought to the attention of all staff members and are refresher training sessions given regularly?	Yes /No

2. Physical security

	Location of server and network infrastructure etc.	
3.	Is an inventory of all IT hardware maintained?	Yes /No
4.	If you have a server, is it located in a secure, locked environment e.g. a dedicated comms room, which is only accessible by authorised staff?	Yes /No
5.	Are your network switches and similar devices located in secure, locked data cabinets?	Yes /No
6.	Are the keys for all data cabinets retained by the principal or school office?	Yes /No

3. Basic network security

	Network hardware	
7.	Are all your network switches, routers, Wi-Fi controllers running the latest firmware provided by the vendor?	Yes /No
	Broadband links	
8.	Are all broadband links connecting the school to the internet provided solely by the PDST?	Yes /No
	Firewall	
9.	Do you have a firewall device to block/control network traffic between the school and the internet (in addition to the PDST firewall)?	Yes /No
10.	If so, is the firewall running the latest firmware?	Yes /No
11.	Is the firewall configured to block/control both inbound and outbound traffic?	Yes /No
12.	Are the firewall logs regularly monitored and any attempted intrusions investigated?	Yes /No
	IP addressing	
13.	Are all your network infrastructure devices such as firewalls, switches, servers etc. configured with static IP addresses and are these addresses recorded in a central database or spreadsheet?	Yes /No
	Wi-Fi	
14.	If you have Wi-Fi in place, is it configured with at least WPA2 encryption (preferably WPA2-Enterprise)?	Yes /No

15.	Are the passwords used to connect to the Wi-Fi network suitably complex that they cannot be guessed by students or others (except where students are permitted access via Wi-Fi)?	Yes /No
16.	Are staff aware that under no circumstances should they divulge Wi-Fi or other passwords to students or guests?	Yes /No
17.	Are the usernames and passwords used to access the Wi-Fi management console or individual access points recorded and stored securely, preferably in the school safe or similar?	Yes /No
	Remote access	
18.	Do you use a virtual private network (VPN) for secure remote access to the school?	Yes /No
19.	Can staff, students, parents or the public access school IT resources e.g. Eportal, directly from the internet?	Yes /No
20.	Are logs kept of both successful and failed attempts to gain remote access to the school's IT systems and resources?	Yes /No
21.	If so, are these logs monitored regularly for attempted intrusions?	Yes /No

4. Server configuration

	Hardware	
22.	Are the server's disks configured with RAID to prevent individual disk failure from halting the server?	Yes /No
23.	Is your server protected by a UPS (battery backup) to protect against power failure and to allow them to graceful shutdown?	Yes /No
	Operating system	
24.	Is your server running a recent version of the operating system (preferably Windows Server 2016) and not Windows Server 2003 or earlier?	Yes /No
25.	Is your server updated with all the latest patches from Microsoft, including the recent patches for the Meltdown and Spectre vulnerabilities?	Yes /No
	Anti-virus	
26.	Are you running anti-virus on your server (this will likely require a different anti-virus software version and configuration than you use on standard PCs)?	Yes /No

	File security	
27.	Are adequate security restrictions (ACLs) in place on both folders and shares to stop unauthorised access to restricted data e.g. sensitive data, staff files etc.?	Yes /No
	Backups	
28.	Is your server backed up to a dedicated external device e.g. a NAS unit, each day?	Yes /No
29.	Is your backup device remote from the server i.e. in a different part of the school, so that it will not be damaged by any fire/flood/theft which may affect the server itself?	Yes /No
30.	Is the backup device stored in a secure environment e.g. a lockable data cabinet or similar?	Yes /No
31.	Are your backups automated so they run without human intervention?	Yes /No
32.	Are your backups monitored on a daily basis to ensure they are successful?	Yes /No
33.	Are any backups taken off-site or to the "cloud"?	Yes /No

5. PC and notebook configuration

	Operating system	
34.	Are all of your PCs and notebooks running a minimum of Windows 7?	Yes /No
35.	Are your PCs and notebooks updated with the latest service packs and patches from Microsoft?	Yes /No
36.	Is the Windows firewall enabled on all PCs and notebooks?	Yes /No
37.	Are staff, students and guests prevented from making changes to the operating system e.g. network settings, screen savers, etc.?	Yes /No
	Access control	
38.	Are all PCs and notebooks members of a Windows *domain* to control access?	Yes /No
39.	If for some reason PCs cannot be joined to a domain, is some other means used to control access to the computers e.g. local user accounts with password protection?	Yes /No
	Anti-virus	
40.	Are you running anti-virus software, with automatic updating of virus signatures, on all of your PCs and notebooks?	Yes /No

41.	Is malware scanning/blocking enabled in your anti-virus software configuration?	Yes /No
42.	Is the anti-virus status of all the school's PCs and notebooks regularly monitored via a central management application (normally provided free by software vendor)?	Yes /No
	Software installation	
43.	Do you have a security policy in place to control the downloading and installation of software by staff members?	Yes /No
44.	Are students and guests restricted from installing software on your PCs and notebooks?	Yes /No

6. Tablet configuration

	Operating system	
45.	If you are using tablet PCs, are they running the latest version of the operating system provided by your vendor?	Yes /No
46.	Are tablets updated with the latest patches from the vendor?	Yes /No
	Anti-virus	
47.	On Android tablets specifically, are you running anti-virus/anti-malware software with automatic updating of virus signatures?	Yes /No

7. User accounts and passwords

	Administrator and privileged accounts	
48.	Is the Windows domain **administrator** renamed and a complex password set? The details should be recorded and stored securely, preferably in the school safe or similar.	Yes /No
49.	Are *individual* accounts granted privileged access rather than using the default administrator account for server management?	Yes /No
50.	Are the details of who has privileged access recorded and review regularly?	Yes /No
51.	Are the passwords for the local administrator accounts on each PC and/or other access control passwords recorded and stored securely, preferably in the school safe or similar?	Yes /No

	Staff and student accounts	
52.	Does each staff member and student have their own personal user account?	Yes /No
53.	Are staff and student accounts disabled or deleted once they leave the school?	Yes /No
	Password policy	
54.	Do you have a password which enforces a minimum of eight alphanumeric characters that are changed every 90 days?	Yes /No

8. Sensitive and personal data

	Enabled devices	
55.	Are devices such as CD/DVD writers or USB drives disabled on all PC and notebooks?	Yes /No
	Storage encryption	
56.	Are the hard disks on PCs and notebooks which contain sensitive data encrypted? Sensitive data includes student details, staff details, medical, HR, financial, payroll and other records.	Yes /No
57.	Are any external disks or memory sticks which are used to store or backup sensitive data encrypted?	Yes /No
	Email encryption	
58.	Is email encryption used to send sensitive documents?	Yes /No

9. Guest/visitor access

	Controlling access	
59.	If you permit guest access to your network, either via Wi-Fi or a cabled connection, is the guest network traffic separated from the main school network?	Yes /No
60.	Do you have a minimum configuration that each guest's PC must meet e.g. Windows 7, current anti-virus software installed?	Yes /No

10. GDPR

61.	Has the school's data protection policies been updated to ensure it complies with the introduction of the General Data Protection Regulation in May 2018 and to ensure all data is held securely e.g. backups, passwords, security, data portability?	Yes /No

11. Insurance Cover

62.	Is the school aware that they can mitigate against some of the financial risks associated with cyber activity and data protection by taking out insurance cover?	Yes /No

Louise McNamara, Director,
Financial Support Services Unit.
28 February 2018

FSSU
Financial Support Services Unit

Teach Emmet, Baile an Mhuilinn, Baile Átha Cliath 14
Teil: 01 2690677 R-phost: info@fssu.ie

Treoirlíne Airgeadais 2017/2018 - 17

Pobalscoileanna, Scoileanna Cuimsitheacha agus Meánscoileanna Deonacha

Seicliosta maidir le hInfreastruchtúr TF

Réamhrá:

Tar éis do roinnt ceisteanna slándála maidir le teicneolaíocht faisnéise (TF) a theacht chun solais i scoileanna le déanaí, tá an seicliosta seo a leanas curtha le chéile againn le híosriachtanais a leagan síos. Ba chóir na híosriachtanais seo a chomhlíonadh le hinfreastruchtúr TF cothrom le dáta, slán, iontaofa a fheidhmiú do mheánscoileanna.

Is éard is aidhm leis an seicliosta seo ná cabhrú leat sainaithint a dhéanamh ar aon cheisteanna a gcaithfear dul i ngleic leo agus eolas maidir leis an dea-chleachtas a chur ar fáil duit. Tá sé tábhachtach go dtuigfeá, áfach, nach sásaíonn sé an gá le measúnacht mhionsonraithe ar do chuid infreastruchtúir, rud ba chóir do do sholáthraí seirbhíse TF a dhéanamh.

Má tá sé ag dul deacair ort aon cheann de na ceisteanna a fhreagairt, ba chóir go mbeadh do sholáthraí seirbhíse TF in ann lámh chúnta a thabhairt duit.

1. Polasaithe

	Polasaí úsáide	
1.	An bhfuil treoirlínte úsáide ríomhairí i bhfeidhm ag do scoil agus an bhfuil cothrom le dáta? I measc na ngnáthpholasaithe tá: • Polasaí Úsáide Inghlactha • Polasaí Rochtana Idirlín • Polasaí Ríomhphoist agus Cumarsáide • Polasaí Slándála Líonra • Polasaí Rochtana Cianda • Polasaí 'Beir leat do Ghléas Féin' (BYOD) • Polasaí Criptiúcháin • Polasaí Príobháideachais	Tá/Níl

2.	An é go bhfuil na treoirlínte curtha ar a súile do na baill foirne go léir agus go dtugtar seisiúin oiliúna athnuachana go rialta?	Is é/Ní hé

2. Slándáil fhisiciúil

	An áit a bhfuil na freastalaithe agus an t-infreastruchtúr líonra, srl.	
3.	An gcoinnítear liosta de na crua-earraí TF ar fad?	Coinnítear/ Ní choinnítear
4.	Má tá freastalaí agat, an bhfuil sé i dtimpeallacht shlán a bhíonn faoi ghlas (m.sh. seomra cumarsáide ar leith) nach bhfuil rochtain ach ag baill foirne údaraithe uirthi?	Tá/Níl
5.	An bhfuil do lasca líonra agus gléasanna den chineál céanna i gcaibinéid sonraí shlána a bhíonn faoi ghlas?	Tá/Níl
6.	An gcoinníonn an príomhoide nó oifig na scoile na heochracha le haghaidh na gcaibinéad sonraí?	Coinníonn/ Ní choinníonn

3. Slándáil bhunúsach líonra

	Crua-earraí líonra	
7.	An bhfuil na dochtearraí is déanaí arna gcur ar fáil ag an díoltóir suiteáilte ar na lasca líonra, ródairí, rialaitheoirí Wi-Fi uile atá agat?	Tá/Níl
	Naisc leathanbhanda	
8.	An é an PDST, agus an PDST amháin, a sholáthraíonn na naisc leathanbhanda uile a úsáidtear leis an scoil a nascadh leis an Idirlíon?	Is é/Ní hé
	Balla Dóiteáin	
9.	An bhfuil gléas balla dóiteáin agat le bac a chur ar thrácht líonra/trácht líonra a rialú idir an scoil agus an tIdirlíon (chomh maith le balla dóiteáin an PDST)?	Tá/Níl
10.	Má tá, an bhfuil na dochtearraí is déanaí suiteáilte ar an mballa dóiteáin?	Tá/Níl
11.	An bhfuil an balla dóiteáin cumraithe le bac a chur ar thrácht/trácht a rialú agus é ag teacht isteach agus ag dul amach?	Tá/Níl
12.	An ndéantar monatóireacht ar logaí an bhalla dóiteáin go rialta agus an ndéantar aon iarrachtaí le briseadh isteach a fhiosú?	Déantar/ Ní dhéantar
	Seoltaí IP	
13.	An bhfuil do ghléasanna infreastruchtúir líonra ar fad, amhail ballaí dóiteáin, lasca, freastalaithe, srl., cumraithe le seoltaí statacha IP agus an bhfuil na seoltaí sin breactha síos i mbunachar sonraí lárnach nó i scarbhileog?	Tá/Níl

	Wi-Fi	
14.	Má tá Wi-Fi i bhfeidhm agat, an bhfuil sé cumraithe le criptiúchán WPA2 ar a laghad (WPA2-Enterprise más féidir)?	Tá/Níl
15.	An bhfuil na pasfhocail a úsáidtear le nascadh le líonraí Wi-Fi casta a ndóthain le nach mbeidh scoláirí ná daoine eile in ann buille faoi thuairim a thabhairt orthu (seachas scoláirí a bhfuil cead acu an Wi-Fi a úsáid)?	Tá/Níl
16.	An eol do bhaill foirne nach ceadmhach dóibh na pasfhocail don Wi-Fi ná pasfhocail eile a thabhairt do scoláirí ná d'aíonna in aon chás?	Is eol/Ní heol
17.	An bhfuil na hainmneacha úsáideora agus na pasfhocail a úsáidtear le rochtain ar an gconsól bainistíochta Wi-Fi nó ar phointí rochtana ar leith breactha síos agus stóráilte go slán sábháilte, i dtaisceadán na scoile nó áit den chineál céanna más féidir?	Tá/Níl
	Rochtain chianda	
18.	An úsáideann tú líonra príobháideach fíorúil (VPN) i gcomhair rochtain chianda shlán ar an scoil?	Úsáideann/ Ní úsáideann
19.	An féidir le baill foirne, scoláirí, tuismitheoirí nó an pobal i gcoitinne rochtain ar acmhainní TF go díreach ón Idirlíon, m.sh. Eportal?	Is féidir/ Ní féidir
20.	An gcoinnítear logaí ar iarrachtaí le rochtain ar chórais agus acmhainní TF de chuid na scoile, beag beann ar cibé acu a n-éiríonn nó nach n-éiríonn leo?	Coinnítear/ Ní choinnítear
21.	Má choinnítear, an ndéantar monatóireacht ar na logaí sin go rialta le haon iarrachtaí le briseadh isteach a bhrath?	Déantar/ Ní dhéantar

4. Cumraíocht an fhreastalaí

	Crua-Earraí	
22.	An bhfuil dioscaí an fhreastalaí cumraithe le RAID ionas nach dteipfidh ar an bhfreastalaí iomlán má theipeann ar cheann de na dioscaí?	Tá/Níl
23.	An bhfuil do fhreastalaí faoi chosaint ag UPS (cadhnra cúltaca) le cosaint i gcoinne cliseadh cumhachta agus le deis a thabhairt dó múchadh go slán?	Tá/Níl
	Córas oibriúcháin	
24.	An bhfuil leagan nua go leor den chóras oibriúcháin suiteáilte ar do fhreastalaí (Windows Server 2016 más féidir) agus ní Windows Server 2003 nó níos sine?	Tá/Níl

25.	An bhfuil na paistí is déanaí ar fad ó Microsoft suiteáilte ar do fhreastalaí, lena n-áirítear na paistí a eisíodh le déanaí i dtaca leis na fabhtanna darb ainm Meltdown agus Spectre?	Tá/Níl
	Frithvíreas	
26.	An bhfuil bogearraí frithvíreas ag rith ar do fhreastalaí (tá gach cosúlacht ar an scéal go mbeadh leagan agus cumraíocht dhifriúil de na bogearraí frithvíreas ag teastáil ná iad siúd a úsáidtear ar ghnáthríomhairí)?	Tá/Níl
	Slándáil comhad	
27.	An bhfuil sriantaí slándála leordhóthanacha (liostaí rialaithe rochtana/ACLanna) i bhfeidhm ar fhillteáin agus tiomántáin chomhroinnte le cosc a chur ar rochtain neamhúdaraithe ar shonraí srianta, m.sh. sonraí rúnda, comhaid ball foirne, srl.?	Tá/Níl
	Cúltacaí	
28.	An ndéantar do fhreastalaí a chúltacú gach lá chuig gléas seachtrach tiomnaithe, m.sh. gléas NAS?	Déantar/ Ní dhéantar
29.	An bhfuil do ghléas cúltacaithe coinnithe amach ón bhfreastalaí, .i. in áit eile sa scoil, ionas nach ndéanfar damáiste dó i gcás dóiteáin/tuile/gada a d'fhéadfadh cur isteach ar an bhfreastalaí féin?	Tá/Níl
30.	An gcoinnítear an gléas cúltacaithe i dtimpeallacht shlán, m.sh. i gcaibinéad sonraí is féidir a chur faoi ghlas nó a leithéid?	Coinnítear/ Ní choinnítear
31.	An bhfuil an próiseas cúltacaithe uathoibrithe ionas go ritheann siad gan gá d'aon duine aon rud a dhéanamh?	Tá/Níl
32.	An ndéantar monatóireacht ar do chuid cúltacaí ar bhonn laethúil lena chinntiú go n-éiríonn leo?	Déantar/ Ní Dhéantar
33.	An gcoinnítear aon chúltacaí lasmuigh den láthair nó sa “néal”?	Coinnítear/ Ní choinnítear

5. Cumraíocht ríomhairí deisce agus glúine

	Córas oibriúcháin	
34.	An bhfuil Windows 7 ar a laghad ar gach ceann de do chuid ríomhairí deisce agus glúine?	Tá/Níl
35.	An ndéantar ríomhairí deisce agus glúine de do chuid a nuashonrú leis na pacaí seirbhíse agus paistí is déanaí ó Microsoft?	Déantar/ Ní dhéantar

36.	An bhfuil Balla Dóiteáin Windows cumasaithe ar gach ríomhaire deisce agus glúine?	Tá/Níl
37.	An gcuirtear cosc le baill foirne, scoláirí agus aíonna athruithe a dhéanamh ar an gcóras oibriúcháin, m.sh. socruithe líonra, spárálaí scáileáin, srl.?	Cuirtear/ Ní chuirtear
	Rialúchán rochtana	
38.	An bhfuil gach ríomhaire deisce agus glúine ina bhall *d'fhearann* Windows le rochtain a rialú?	Tá/Níl
39.	Mura féidir ríomhairí áirithe a nascadh le fearann ar chúis éigin, an ndéantar rochtain ar na ríomhairí a rialú ar bhealach eile, m.sh. úsáideoirí áitiúla a bhfuil pasfhocal acu?	Déantar/ Ní dhéantar
	Frithvíreas	
40.	An bhfuil bogearraí frithvíreas suiteáilte ar gach ríomhaire deisce agus glúine agus an bhfuil nuashonrú uathoibríoch sínithe víris ina chuid de na bogearraí sin?	Tá/Níl
41.	An bhfuil scanadh le haghaidh bogearraí mailíseacha cumasaithe i do bhogearraí frithvíreas?	Tá/Níl
42.	An ndéantar monatóireacht go rialta ar stádas frithvíris na ríomhairí deisce agus glúine uile ar leis an scoil iad trí fheidhmchlár bainistíochta lárnaí (rud is iondúil a chuireann díoltóir bogearraí ar fáil saor in aisce)?	Déantar/ Ní dhéantar
	Suiteáil bogearraí	
43.	An bhfuil polasaí slándála i bhfeidhm agat le híoslódáil agus suiteáil bogearraí ag baill foirne a rialú?	Tá/Níl
44.	An é nach féidir le scoláirí ná aíonna bogearraí a shuiteáil ar ríomhairí deisce ná glúine de do chuid?	Is é/Ní hé

6. Cumraíocht táibléad

	Córas oibriúcháin	
45.	Má tá ríomhairí táibléid á n-úsáid agat, an bhfuil an leagan is déanaí den chóras oibriúcháin arna chur ar fáil ag do dhíoltóir suiteáilte orthu?	Tá/Níl
46.	An ndéantar na táibléid a nuashonrú leis na paistí is déanaí ón díoltóir?	Déantar/
	Frithvíreas	
47.	I gcás táibléid Android go sonrach, an bhfuil bogearraí frithvíreas/frith-bhogearraí mailíseacha suiteáilte orthu agus an bhfuil nuashonrú uathoibríoch sínithe víris ina chuid de na bogearraí sin?	Tá/Níl

7. Cuntais úsáideora agus pasfhocail

	Cuntais riarthóra agus faoi phribhléid	
48.	An bhfuil an **riarthóir** fearainn Windows athainmnithe agus pasfhocal casta socraithe? Ba cheart na sonraí sin a bhreacadh síos agus a stóráil go slán, i dtaisceadán na scoile nó a leithéid más féidir.	Tá/Níl
49.	An dtugtar rochtain faoi phribhléid do chuntais úsáideora *aonair* seachas don chuntas riarthóra réamhshocraithe i gcomhair bainistíocht freastalaí?	Tugtar/ Ní thugtar
50.	An é go mbreactar síos cé na daoine a bhfuil rochtain faoi phribhléid acu agus go ndéantar athbhreithniú ar an bhfaisnéis sin go rialta?	Is é/Ní hé
51.	An é go mbreactar síos na pasfhocail le haghaidh na gcuntas riarthóra áitiúil ar gach ríomhaire agus/nó pasfhocail rialúcháin rochtana eile agus go ndéantar iad a stóráil go slán, i dtaisceadán na scoile nó a leithéid más féidir?	Is é/Ní hé
	Cuntais na mball foirne agus na scoláirí	
52.	An bhfuil a chuntas pearsanta féin ag gach ball foirne agus scoláire?	Tá/Níl
53.	An ndéantar cuntais ball foirne agus scoláirí a dhíchumasú nó a scriosadh a luaithe a fhágann siad an scoil?	Déantar/ Ní dhéantar
	Polasaí maidir le pasfhocail	
54.	An bhfuil córas i bhfeidhm lena chinntiú go mbíonn ocht gcarachtar alfa-uimhriúla ar a laghad i ngach pasfhocal agus go n-athraítear gach 90 lá é?	Tá/Níl

8. Sonraí íogaire agus pearsanta

	Gléasanna cumasaithe	
55.	An bhfuil gléasanna amhail scríbhneoirí CD/DVD nó tiomántáin USB díchumasaithe ar gach ríomhaire deisce agus glúine?	Tá/Níl
	Criptiúchán stórais	
56.	I gcás ríomhairí deisce agus glúine a bhfuil sonraí íogaire orthu, an bhfuil na dioscaí crua criptithe? Is éard atá i gceist le sonraí íogaire ná sonraí faoi scoláirí agus baill foirne, chomh maith le taifid leighis, AD, airgeadais, párolla agus taifid eile.	Tá/Níl
57.	I gcás dioscaí seachtracha nó flaistiomántáin a úsáidtear le sonraí íogaire a stóráil nó a chúltacú, an bhfuil siad criptithe?	Tá/Níl

	Criptiúchán r-phoist	
58.	An úsáidtear criptiúchán r-phoist le doiciméid íogaire a sheoladh?	Úsáidtear/ Ní úsáidtear

9. Rochtain d'aíonna/do chuairteoirí

	Rochtain a rialú	
59.	Má cheadaíonn tú d'aíonna rochtain ar do líonra, cibé trí Wi-Fi nó trí chábla, an gcoinnítear trácht na n-aíonna scartha ó phríomhlíonra na scoile?	Coinnítear/ Ní choinnítear
60.	An éilíonn tú go sásaíonn ríomhaire an aoi íosriachtanais, m.sh. Windows 7, bogearraí frithvíreas atá cothrom le dáta suiteáilte?	Éilíonn/ Ní éilíonn

10. An Rialachán Ginearálta maidir le Cosaint Sonraí (GDPR)

61.	An bhfuil polasaithe cosanta sonraí na scoile tugtha suas chun dáta lena chinntiú go mbeidh siad in oiriúint leis an Rialachán Ginearálta maidir le Cosaint Sonraí, a thabharfar isteach i mí na Bealtaine 2018 agus lena chinntiú go gcoinnítear gach sonra go slán, m.sh. cúltacaí, pasfhocail, slándáil, iniomparthacht sonraí?	Tá/Níl

11. Clúdach árachais

62.	An eol don scoil gur féidir roinnt de na rioscaí a bhaineann le cibearbhagairtí agus cosaint sonraí a mhaolú ach árachas a ghlacadh?	Is eol/Ní eol

Louise McNamara, Stiúrthóir,
An tAonad um Sheirbhísí Tacaíochta Airgeadais.
An 28 Feabhra 2018