Disability Sheffield
Centre for Independent Living

Digital Security

A practical guide for Individual Employers

Written by Sirinda Bhandal on behalf of Disability Sheffield

Funded by skillsforcare

Introduction

Individuals who employ personal assistants have a legal responsibility to keep information about their staff safe and secure. Maintaining safe information technology (IT) systems and digital security processes forms part of this.

As an individual employer (IE) you have a responsibility to ensure all devices you use to process, store and send data are adequately protected. Whether you use a smart phone, tablet or a laptop or computer, all of these need to have security in place.

Cyber criminals are getting more and more sophisticated. If your data is not appropriately protected, you are putting yourself and your employees at risk of becoming victims of cyber crime or identity fraud.

Please consider for a moment...if your smart phone is stolen, think about all the information you store on there - not just your information, but that of your PAs too.

Leaving your smart phone unlocked is like leaving your front door open - password protecting it is just one way of securing it. Read on to find out more.

It is vital that all your digital devices are secure, and that your PAs are trained in all your policies and procedures to maintain security

Purpose of this guide

IEs are able to use improved and secure systems for managing their PAs and sharing information with third parties

- IEs in receipt of a personal health budget, a direct payment or who are self-funded, have more control over ensuring that their home devices are suitable for managing their workforce and they have necessary security in place.
- IEs have the necessary policies and procedures in place for safe storage of data on devices used in the home.

Inside this guide

Section one

In this section we look at the devices you use to store data and how to ensure they are safe and secure.

Device security

Whether you use a phone, tablet, laptop or computer, this section provides practical advice on how to secure these devices.

Password security

The main purpose of a password is to prevent unauthorised access to your devices and information. This section provides advice on how to securely manage your passwords and user accounts.

Section two

Digital policies and procedures

This section looks at what policies and procedures you need in place to effectively manage your devices and your PAs access to these devices.

Section three

Online systems to help you more securely manage your PAs.

Reviews of online systems to help manage rotas and send out alerts to your PAs.

Section four

Security software

A list of products to help protect your devices.
* We are not recommending any particular product we suggest you get specialist advice on the product's suitability for your particular needs.

Resources

Further help and information and advice.

Glossary of terms

Digital Security

Digital security is all about ensuring the devices you use to store data are safe and secure. This could be your smart phone, tablet or your laptop or computer.

As an IE you will be storing data relating to your PAs and so you have a responsibility to ensure you put the necessary security precautions in place.

1. Device Security

Whether you use a smart phone, tablet, laptop or computer to store, send and receive data about yourself and your employees, you should ensure these are properly protected.

Anti-virus software protects your devices from becoming infected by malicious programmes and viruses, designed to cause problems for your devices. If you install anti-virus software you must also make sure it is regularly updated.

Top security tips for your digital devices

We are not recommending any particular products throughout this guide and we recommend you get specialist advice on the product's suitability for your particular needs. Please see page ten for a list of suggested products.

Protecting your devices

Always install anti-virus software on your computers, tablets and smart phones, and make sure these are regularly updated. Make sure all your phones, tablets and laptops are password protected.

Backing up your data

If you are storing important information on your devices it is vital that this data is backed up. If you don't you could lose this information if your device is lost, stolen or becomes unusable e.g. from a virus infection or gets damaged.

Backing your data to the cloud is usually the safest option. Not only does it provide you with the added advantage of being able to access your information from any device with an internet connection, it also provides you with an easy way to restore your data if you need to.

Many smart phones come with free online back-up services already pre-installed and set-up for you. Check whether yours does, and make sure it is switched on to automatically back-up.

You can also back-up your device to a portable memory device (eg like an external computer hard drive or a USB memory stick). To do this you would simply copy your data to the memory device and then store it securely.

Storing your information online

Consider whether to use a cloud service provider to store all your documents, Google Drive or Office 365 are two options, but there are many more available.

These cloud service providers, provide a private password protected space that only you can access, or other people you have given permission to, to store your data. Similar to the benefits of backing up online, having your data in the cloud means it is accessible at all times from any device with an internet connection.

Consider encryption for highly sensitive data

If you hold a lot of sensitive data on your device, you could consider encryption. Encryption is a means of turning your data into unreadable code that can only be opened by authorised users.

Make sure data is completely deleted

If you dispose of an old computer, laptop, tablet or phone, make sure the data you hold has been completely deleted. Using the standard 'delete' option does not fully remove all data.

2. Password security

In today's world we use passwords for everything, from online banking to online shopping, and for accessing our computer, laptop, tablet or phones.

Why you shouldn't share passwords

The purpose of passwords is to protect your device, data and your different online accounts from unauthorised use. That is why it is so important never to share your passwords with anyone else.

However we appreciate, sometimes PAs carry out for work for an IE that requires the use of their password. You may give them your account details for example in order to carry out online shopping on your behalf.

If you do share passwords with your PA, make sure you have an agreement in place that will clearly set out how they must protect the information they have access to during their employment with you.

Setup a separate account for your PA

If you can, it is always better to set-up a separate account for your PA using your bank details, to allow you to track everything they have purchased under that account name. This is particularly important if you have multiple PAs doing the same task for you. Online shopping accounts do allow for multiple users - check with your bank and ask whether they are willing do the same.

Top Password tips

- Never click yes on websites to auto-save your log-in details - this leaves your account vulnerable and open to misuse by an unauthorised user.
- Change all your passwords whenever a PA leaves you - otherwise they could continue to access your accounts once they have left your employment.
- Never use public wifi to access your bank account or websites containing sensitive information, and make sure your employees don't either. Malicious software can be used to track your key strokes and record your passwords. Criminals can then use this information to gain access to your accounts.
- When setting up a password, include combination of multiple words, characters and numbers (but not your date of birth).
- Consider using software to hold all your passwords securely - these are called Password Manager applications, and can be helpful if you have multiple log-ins and passwords to remember.

3. Sharing data electronically

As IEs you may have to send confidential documents to the local authority, Clinical Commissioning Group, the NHS and other agencies, eg payroll agencies.

Should sensitive information be sent via email?

You should be aware that email is not a particularly secure way of sending information – it can be easy to intercept or can be sent to the wrong person in error. You could consider using an encrypted email service. Ask the agency who are requesting this information whether they can provide this for you.

Password protecting documents

Another way of securing information held in a document is to password protect it. Most office applications provide this facility. When you go to save your document, there will usually be an options tab available. Clicking on this should provide you with the facility to password protect your document.

We recommend

Confidential information sent via email should always be password protected. Should you inadvertently send the email to the wrong person, they won't be able to open the attachment without the password you provide. You can then telephone the person to inform them of the password required to open the document.

Digital policies and procedures

Policies and procedures are sets of rules you expect your PAs to follow, and they also set out how you will manage your IT and digital security.

We recommend - As an IE it is recommended that you put the following IT policies and procedures in place to protect you and your employees.

1. Digital Security Policy

A Digital or IT Security Policy will set out the security measures you have put in place to protect your devices, which are all covered in section one of this guide.

It will contain things like informing PAs that your devices are password protected, have anti-virus software installed, and what behaviour is expected to maintain your standards and to ensure security of your devices.

2. Acceptable Use Policy

Why do I need an Acceptable Use Policy?

An Acceptable Use Policy is a set of rules that will define how your PAs can use your devices and what is expected from them whilst employed by you. It will set out how they should use your devices and should also cover things like how they are expected to use email and the internet.

It should also contain guidance on how and where they should save data. For example, if you don't want your PAs to hold information about you on their personal devices, then this should be detailed in this policy.

It should also set out things like not using your devices for personal use.

You need to decide what you think is acceptable use, and then create a policy based on this. It is important this is covered during the training and induction of your PA and referenced in their job description too.

If your PAs go against what is set out in your policy and misuse your devices, then you have grounds to start disciplinary procedures.

3. Inducting and training your staff

The above policies should be put in place and explained during induction and training. It is important your PAs understand what they can and can't do with regards to using your devices at work.

4. Job descriptions for your PAs

You need to ensure that all PAs with responsibility for using your devices have these duties clearly set out in their job descriptions, and that they also reference the appropriate policy guidance.

5. When PAs leave

It is also a good idea to have a checklist of procedures, for instance removing their access to your devices and online applications.

It will include things like deleting their user accounts and changing any passwords they may have had access to during their employment with you.

Digital security
Staff awareness is your best line of defence.

Online systems for managing PAs

There are a number of online systems to manage staff and rota's. Some applications you need to pay for, but there are free tools you can use too.

Below are some examples. We are not recommending any particular products throughout this guide and recommend you get specialist advice on the product's suitability for your particular needs.

Google Calendars to manage rotas

Google provides a free online calendar which you can share with your employees. You could create a master copy but give your employees edit rights, so they can complete which shifts they can do in real time.

You can also send messages out to all your PAs via your Google environment, for example, should you need to contact them all quickly to fill a shift.

Make sure you always log out

If you do use online email systems to send potentially sensitive information about yourself and your employees, make sure you always log out afterwards. If you leave your online systems logged on, other people could access your accounts. Make sure any PAs who have access to these accounts are also reminded to log out after use.

Review of different rota management software

Sheffield Volunteer Centre have reviewed different software for managing volunteers that can also be used to manage staff too.

www.sheffieldvolunteercentre.org.uk/software-for-managing-volunteer-shifts-or-online-rotas

Deputy

This rota management software can be used to manage shifts and allocate tasks to employees. You set up shifts and other team members receive alerts if they can do it, with a confirmation added. You can also set up tasks for them to complete during their shifts. Deputy also offers payroll integration too.

It looks easy and simple to set up, and there is an app you can download for your smart phone too. There is a small monthly fee.

You can sign-up for a free trial and try it out using the link below: www.deputy.com

Security software

We are not recommending any particular product below, we recommend you get specialist advice on the product's suitability for your particular needs.

AVAST – Free Anti-virus software

Prevents viruses, scans apps and tells you what they have access to. Detects unsafe websites, can remotely control your tablet to activate siren or delete your data if your device is stolen.
www.avast.com

Folder Lock

Encryption software to turn your data into unreadable code that can only be opened by authorised users.
www.folder-lock.en.softonic.com/

Look out – Malware Protection

Provides malware protection to prevent malicious software infiltrating your computer. www.lookout.com/uk

Alarm security HD – Security for tablets and phones

This software plays a loud alarm if someone tries to steal your device - it can even take a photograph of the thief! May be particularly helpful for users with visual impairments. The alarm can be de-activated by entering a PIN number. https://itunes.apple.com/us/app/alarm-security-hd-ad/id405688386?mt=8

Pass Hub

Password Manager applications help if you have multiple log-ins and passwords to remember. Try www.passhub.net for an easy to use option.

Stash – Secure storage area on your phone or tablet

Store sensitive data securely. Provides a 'safe' for your tablet, storing information into separate boxes within your tablet so it can be held securely. www.stash.global

Carbonite – Cloud back up software

Mobile back-up and security. Remotely access your tablet, activate alarm, and wipe memory. www.carbonite.com

Killdisk – Free data deletion software

Deletes data thoroughly from your hard drive.
www.killdisk.com

Further information and advice

Resources

Digital working, learning and information sharing

Useful information and guidance on cyber security, data sharing and the new General Data Protection Regulation (GDPR).

www.skillsforcare.org.uk/digital

Information Hub for IEs and PAs

This hub provides lots of useful information and advice. It is for people who employ their own care and support staff and the organisations that support them.

www.skillsforcare.org.uk/iepahub

Digital Resource for Carers

Brings together a number of digital products and online resources to help organisations provide comprehensive information and support for carers.

www.carersuk.org/for-professionals/carersuk-products/digital-resource-for-carers

Animation by Flycheese

Short animation which gives some basic information and suggestions to think about regarding data protection and digital security.

https://youtube.com/watch?v=sm9Zeyr4jAI

General staying safe online advice

- Barclays digital safety quiz
  www.barclays.co.uk/security/digitally-safe-quiz/
- Barclays keep your accounts safe
  www.barclays.co.uk/security/keep-your-accounts-safe
- Internet Safety Rule
  www.gov.uk/government/news/dont-ignore-internet-safety-rules
- www.getsafeonline.org
- Digital champions to help you in the home (based in Sheffield)
  www.sheffieldonline.net
- Devil's in your details - a video highlighting cyber crime, and how easy it is to impersonate someone online
  www.youtube.com/watch?v=Ugl8bmZF9Pc
- Password Manager software - This article explains what password manager software is and how it works.
  www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/

Glossary of terms

Anti-virus - a software programme that protects your devices from malicious programmes.

App – short for 'application' which is the same thing as a software programme. While an app may refer to a programme for any hardware platform, it is most often used to describe programmes for mobile devices, such as smart phones and tablets.

Cloud computing - the use of various services, such as software development platforms, servers, storage and software, accessed over the internet, often referred to as the 'cloud'.

Cyber security - defined as the protection of all computer systems, phones, networks and data in cyberspace.

Device – any electronic item, such as a smart phone, tablet, laptop or computer.

Malware – is short for 'malicious software' and is a term used to refer to a variety of hostile or intrusive software, including computer viruses, worms, Trojan horses, spyware, adware, scareware, and other intentionally harmful programmes.

Online back-up - using a third party provider to copy your data over the internet to another computer provided by a cloud computing provider.

Public wifi - wifi means a wireless network over which you would usually access the internet. Public wifi is an unsecured public network. Your internet at home would be set up using a private network.

Smart phone - a mobile phone that performs many of the functions of a computer. The difference between an ordinary mobile phone and a smart phone is that a smart phone typically has a touch screen interface. It can provide Internet access, and an operating system and is capable of running downloaded apps.

Encrypted email service – a way of sending email securely, the message content is unreadable to unauthorised users.

Appendix A

Model Digital Security Policy for Employers

Devices in use

You will have access to phone, tablet, laptop or computer during your employment.

You will be issued with a username and password to use these devices. You must not share these with anyone else.

Antivirus software is installed on all devices and updates regularly. If you spot any errors regarding updates, please alert your employer.

Saving data – all data created during your employment should be saved to one of the devices above.

All our devices are set to back up automatically; you do not need to do anything to back up data.

Password security

In today's world we use passwords for everything, from online banking to online shopping and to access our phones, tablets and computers.

Why you shouldn't share passwords

The purpose of passwords is to protect a device or an account being used by others who do not have permission to do so (an unauthorised user). That is why it is important never to share your passwords with anyone else.

Model Digital Security Policy for Employers continued

Top five Password tips

1. Never click yes to save password on websites, as this leaves your account logged in and open to misuse by an unauthorised user

2. Change all your passwords when your PAs leave, otherwise they could be used to access your accounts, once they have left your employment

3. Never use public WIFI to access your bank account or other sensitive information. Malicious software (e.g. software that brings harm to your computer such as viruses and spyware) can be used to track your key strokes and record your passwords.

4. Use a combination of multiple words, characters and numbers (but not your date of birth)

5. Consider using software to hold all your passwords securely, these are called password manager applications.

Disability Sheffield
Centre for Independent Living

Funded by
skillsforcare

Thank you to members of the Sheffield Individual Employer and PA development group whose experiences and questions formed the basis of this practical guide.

www.disabilitysheffield.org.uk
@disabilitysheff
@sirindabhandal

Digital Security: A practical guide for Individual Employers
Edition 1: May 2018