# Better Security, Better Care

## Data Security and Protection Toolkit (DSPT) Action Plan –

## IT systems and Devices

| Evidence item | Question | Tooltip | Action |
|---|---|---|---|
| **1.6.4** | What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately? | Smartphones are especially vulnerable to being lost or stolen. What has been put in place by your organisation to protect them to prevent unauthorised access? E.g. is there a PIN or fingerprint or facial scan? Is there an app set up to track the location of a lost/ stolen smartphone, and 'wipe' its contents remotely? You may need to ask your IT supplier to assist with answering this question.<br>If your organisation does not use any mobile phones, write "Not applicable" in the text box.<br>Guidance is available from Digital Social Care https://www.digitalsocialcare.co.uk/social-care-technology/mobile-devices/ | 1.6.4 |
| **1.6.6** | If staff, directors, trustees and | The devices referred in this question include laptops, tablets, mobile phones, CDs, USB sticks | 1.6.6 |

| Evidence item | Question | Tooltip | Action |
|---|---|---|---|
| | volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced? | etc. This applies to use of devices whether the person is on duty or not e.g. if they access your system(s) when not on shift. Please upload your Bring Your Own Device policy and any associated guidance, and evidence of how this policy is enforced. If nobody uses their own devices, write “Not applicable” in “Enter text describing document location”. A template Bring Your Own Device (BYOD) policy, and examples of how this policy might be enforced, is available from Digital Social Care https://www.digitalsocialcare.co.uk/social-care-technology/mobile-devices/ | |
| **1.8.3** | What are the top three data and cyber security risks in your organisation and how does your organisation plan to reduce those risks? | All organisations have risks and should be able to identify what they are. Thinking about your responses to all of the questions in the toolkit, consider which three areas carry the most risk for your organisation. Provide a brief headline for each risk and say what your organisation plans to do to reduce that risk. | 1.8.3 |
| **4.1.2** | Does your organisation know who has access to personal and confidential data through its IT system(s)? | Your organisation should know who has access to the personal and confidential data in its IT system(s). Each person needs to have their own account to access a system. If that is not currently possible, and users share a login, the organisation must risk assess the situation and agree a plan to end the use of shared logins. If your organisation does not use any IT systems, then tick and write “Not applicable” in the comments box. | 4.1.2 |

| Evidence item | Question | Tooltip | Action |
|---|---|---|---|
| **4.2.5** | Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles? | When people change roles or leave your organisation, there needs to be a reliable way to amend or remove their access to your IT system(s). This could be by periodic audit to make sure that people's access rights are at the right level. It is important that leavers who had access to personal data have their access rights revoked in line with your policies and procedures. This includes access to shared email addresses.<br>If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box | 4.2.5 |
| **4.3.1** | Have all the administrators of your organisation's IT system(s) signed an agreement to hold them accountable to higher standards? | The people within your organisation who are IT system administrators may have access to more information than other staff. Therefore, they need to be held accountable in a formal way to higher standards of confidentiality than others. This requirement applies to IT system administrators working in external companies who support your organisation's IT systems This formal agreement could be part of a job description or a contract with your IT support company and/or systems supplier/s. If your organisation does not use any IT systems, then 'tick' and write "Not applicable" in the comments box. | 4.3.1 |
| **4.5.4** | How does your organisation make sure that staff, directors, trustees and volunteers use | If your organisation has any IT systems or computers, it should provide advice for setting and managing passwords. Each person should have their own password to access the computer, laptop or tablet that they are using and a separate | 4.5.4 |

| Evidence item | Question | Tooltip | Action |
|---|---|---|---|
| | good password practice? | password for other systems. These passwords should be 'strong' i.e. hard to guess. This could be enforced through technical controls i.e. your system(s) require a minimum number of characters or a mixture of letters and numbers in a password. If your organisation does not use any IT systems, computers or other devices, write "Not applicable" in the text box. Information about good password practice is available from Digital Social Care https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/use-strong-passwords/ | |
| **6.2.3** | Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date? | This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or other devices, then tick and write "Not applicable" in the comments box. Further information is available from Digital Social Care https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/have-up-to-date-antivirus-software/ | 6.2.3 |
| **6.3.2** | Have staff, directors, trustees and volunteers been advised that use of public Wi-Fi for work purposes is unsafe? | Use of public Wi-Fi (e.g. Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) could be unsafe and lead to unauthorised access of personal data. Staff, directors, trustees and volunteers if you have them, should be advised of | 6.3.2 |

| Evidence item | Question | Tooltip | Action |
|---|---|---|---|
| | | this. If nobody uses mobile devices for work purposes out of your building/offices, then tick and write “Not applicable” in the comments box. | |
| **7.3.1** | How does your organisation make sure that there are working backups of all important data and information? | It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation’s back up systems work and how you have tested them.<br>You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or IT systems, write “Not applicable” in the text box.<br>For advice about backups, see Digital Social Care https://www.digitalsocialcare.co.uk/data-security-protecting-myinformation/cyber-security/back-up-your-data/ | 7.3.1 |
| **7.3.2** | All emergency contacts are kept securely, in hardcopy and are up-to-date. | Contacts include phone number as well as email. | |
| **7.3.4** | Are backups routinely tested to make sure that data and information can be restored? | It is important that your organisation’s backups are tested at least annually to make sure data and information can be restored (in the event of equipment breakdown for example). You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or IT systems, then tick and write “Not applicable” in the comments box. | 7.3.4 |
| **8.1.4** | Are all the IT systems and the software | Systems and software that are no longer supported by the manufacturer can be unsafe as they are no | 8.1.4 |

| Evidence item | Question | Tooltip | Action |
|---|---|---|---|
| | used in your organisation still supported by the manufacturer or the risks are understood and managed? | longer being updated to protect against viruses for example. You may need to ask your IT supplier to assist with answering this question. Examples of unsupported software include: Windows XP, Windows Vista, Windows 7, Java or Windows Server 2008. Windows 8.1 is supported until January 2023. Windows 10 is supported and is the most up to date version of Windows. This question also applies to software systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example. If your organisation does not use any IT systems or software, then tick and write "Not applicable" in the comments box. For guidance (including information on how to check which software versions you have), see Digital Social Care. https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-software-updates/ | |
| **8.2.1** | If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk | This is a conscious decision to accept and manage the associated risks of unsupported systems. This document should indicate that your board or management team have formally considered the risks of continuing to use unsupported items and have concluded that the risks are acceptable. If your answer to the previous question was yes, write "Not applicable" in "Enter text describing document location". | 8.2.1 |

| Evidence item | Question | Tooltip | Action |
|---|---|---|---|
| | of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk. | | |
| **8.3.5** | How does your organisation make sure that the latest software updates are downloaded and installed? | It is important that your organisation's IT system(s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any IT systems, devices or software, write "Not applicable" in the text box. Further information is available from Digital Social Care https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-software-updates/ | 8.3.5 |
| **9.1.1** | Does your organisation make sure that the passwords of all networking components, such as | Networking components include routers, switches, hubs and firewalls at all of your organisation's locations. Your organisation may just have a Wi-Fi router. This does not apply to Wi-Fi routers for people working from home. You may need to ask your IT supplier to assist with answering this | 9.1.1 |

| Evidence item | Question | Tooltip | Action |
|---|---|---|---|
|  | a Wi-Fi router, have been changed from their original passwords? | question. If your organisation does not have a network or internet access, then tick and write "Not applicable" in the comments box. |  |
| **10.2.1** | Do your organisation’s IT system suppliers have cyber security certification? | Your organisation should ensure that any supplier of IT systems has cyber security certification. For example, external certification such as Cyber Essentials, or ISO27001, or by being listed on Digital marketplace, or by completing this Toolkit.<br>An IT systems supplier would include suppliers of systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example.<br>If your organisation does not use any IT systems, then tick and write “Not applicable” in the comments box.<br>Guidance is available from Digital Social Care https://www.digitalsocialcare.co.uk/data-security-protecting-myinformation/cyber-security/manage-your-suppliers/ | 10.2.1 |