DSPT Guide

Helping you to evidence good data security standards ahead of your DSPT assessment

PASS

We understand that completing the DSPT can be a daunting task. With dozens of questions relating to each of the 10 National Data Guardian (NDG) data security standards, we have compiled the following guide to help you prepare for some of the more challenging aspects of IT protection.

Are you ready? We can help!

Completing the Data Security Protection Toolkit (DSPT) ensures care providers are taking the right steps towards complying with nationally recognised standards of data security.

PASS can help you prepare the necessary information and evidence so you can complete your DSPT in a timely way. The following guide provides succinct and straightforward points for consideration.

Key areas to consider

- Data access
- Organisational requirements
- Software updates
- Continuity & disaster recovery
- Data protection
- Data security
- Data encryption
- Managing suppliers
- Data on devices
- Personal data
- Data breach
- Ready? Let's go...

Feel free to talk to us for further advice. Just call us on 03300 940 121. We are happy to help.

PASS

Data access

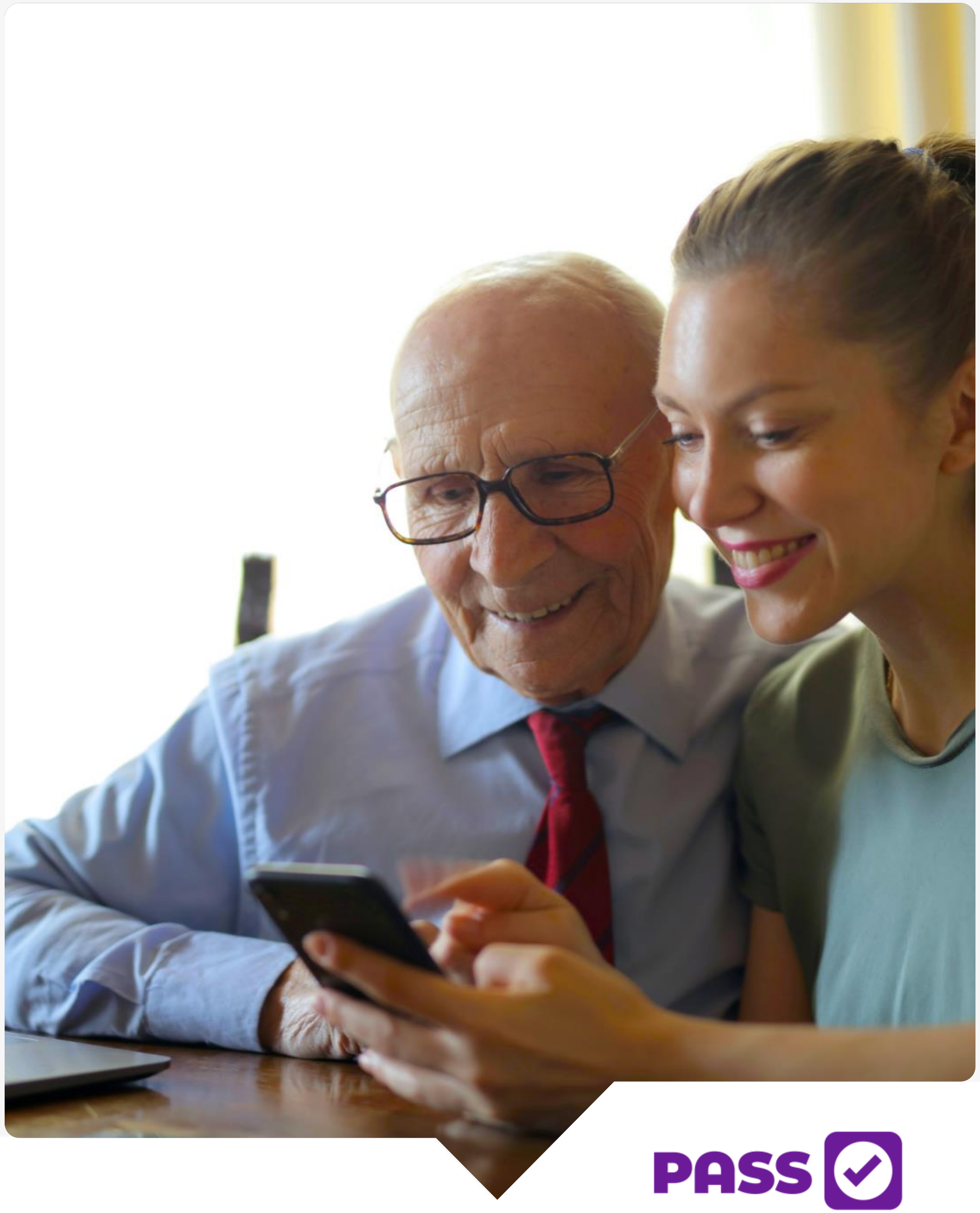
Are the following in place and up to date?

- Your organisation has a reliable way of removing or amending people's access to IT systems when they leave or change roles.
- Your organisation makes sure that staff, directors, trustees and volunteers apply good password practice.
- **TIP:** If your organisation has I.T systems or computers it should provide advice for setting and managing passwords. Each person should have their own password details.

Data protection

Ensure you check that...

- Your organisation has up to date policies in place for data protection and for data and cyber security.
- Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. This type of risk assessment is called a Data Protection Impact Assessment (DPIA).



Data on devices

Can you answer yes to the following?

- Your organisation has a comprehensive process 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. If you allow staff to use their own device, ensure you have a 'bring your own device' policy in place.
- **TIP:** Use a PIN, fingerprint or facial scan to authorise login / use of the device where possible. You can ask your I.T support for help.

Organisational requirements

Has your organisation...

- Assigned the responsibility of data protection to a named person?
- Ensured there is a policy or policies in place to cover: Data Protection, Data Quality, Record Keeping, Data Security and, where relevant, Network Security?
- Designated a Data Protection Officer (DPO)?
- Made sure that the correct Data Protection policies in place.

PASS

Data security

Have you thought about...

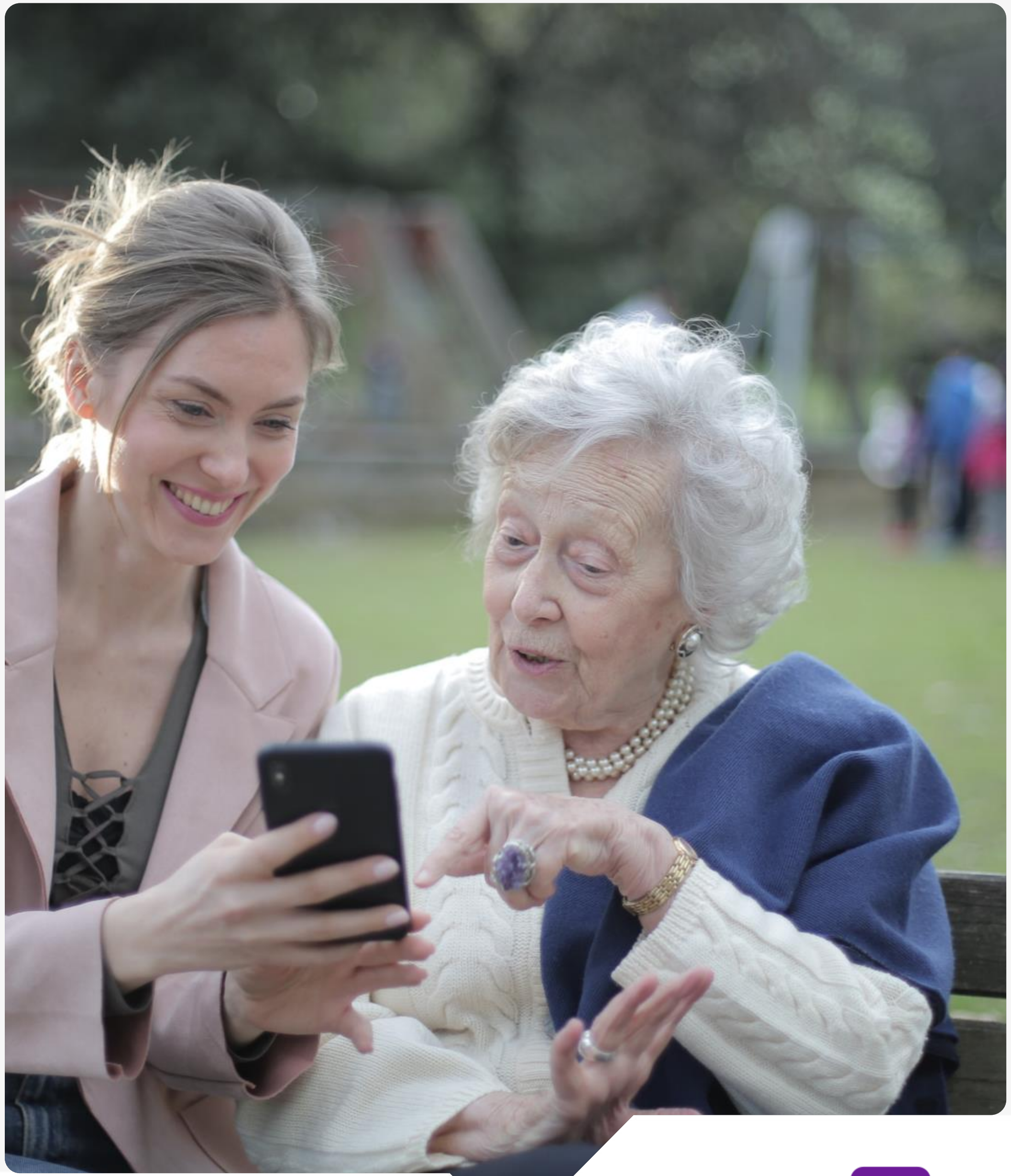
- What the top three data and cyber security risks are in your organisation and how your organisation plan to reduce those risks?
- If your organisation has a timetable which sets out how long you retain all data and records for?
- Ensuring that a flow of all data used within your organisation is mapped out, including who you share data with.

Feel free to talk to us for further advice. Just call us on 03300 940 121. We are happy to help.

Personal data

Have you ensured...

- That you have a record of processing activity (ROPA)?
- You know where all your data is stored?
- Your organisation knows who has access to personal and confidential data through its IT system(s).
- Your organisation's data protection policy describes how you keep personal data safe and secure.



Software updates

Can you answer yes to the following?

- Computers and other devices used across your organisation have antivirus/antimalware software installed and up to date.
- Your organisation makes sure that the latest software updates are downloaded and installed.
- Your organisation ensures that there are working backups of all important data and information. It is important that backups are frequent and successful.
- Backups are routinely tested to make sure that data and information can be restored.

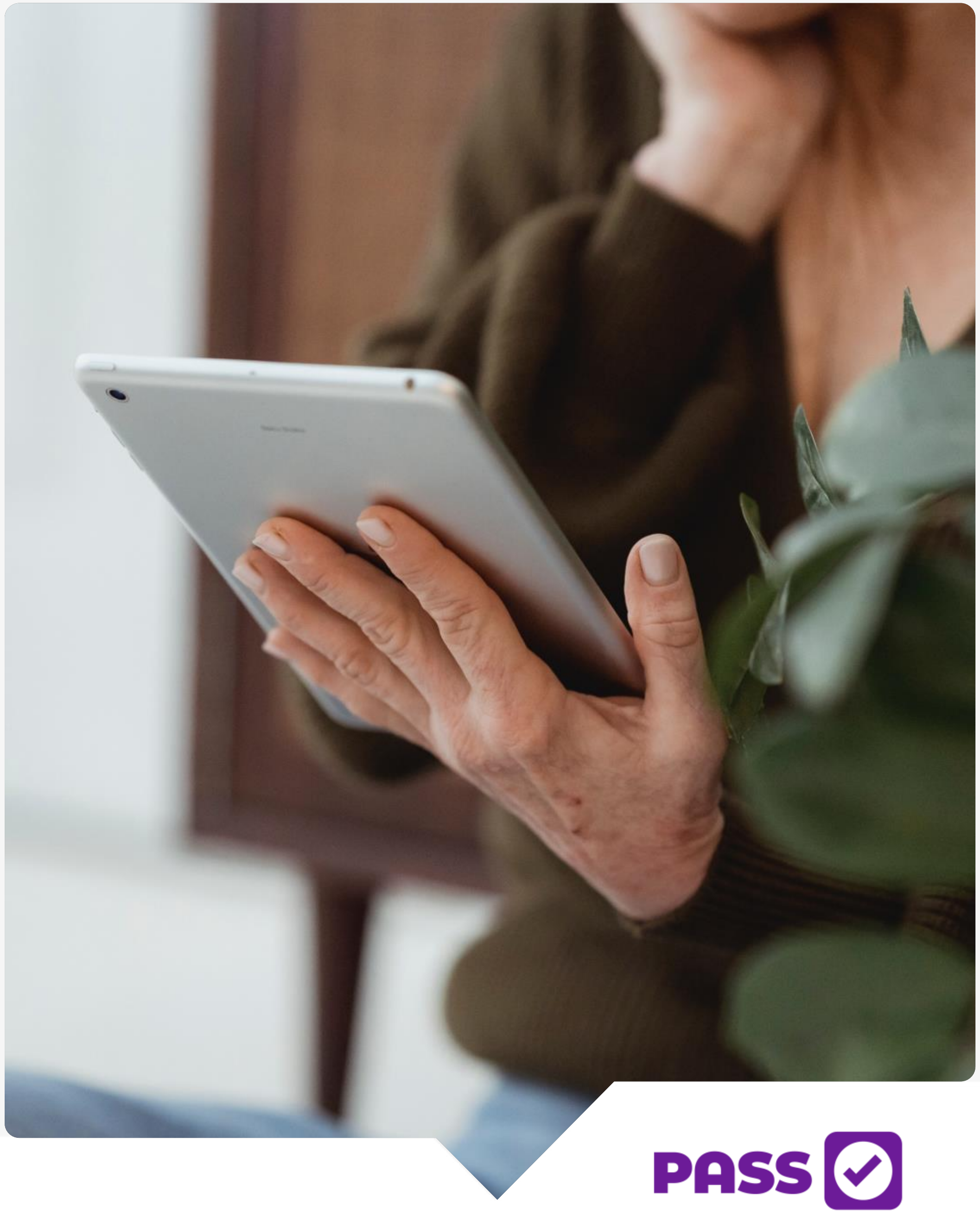
PASS

Feel free to talk to us for further advice. Just call us on 03300 940 121. We are happy to help.

Data encryption

Be sure to check that...

- All laptops and tablets or removable devices that hold or allow access to personal data are encrypted.
- Your encryption protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people.
- Your organisation ensures that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords.

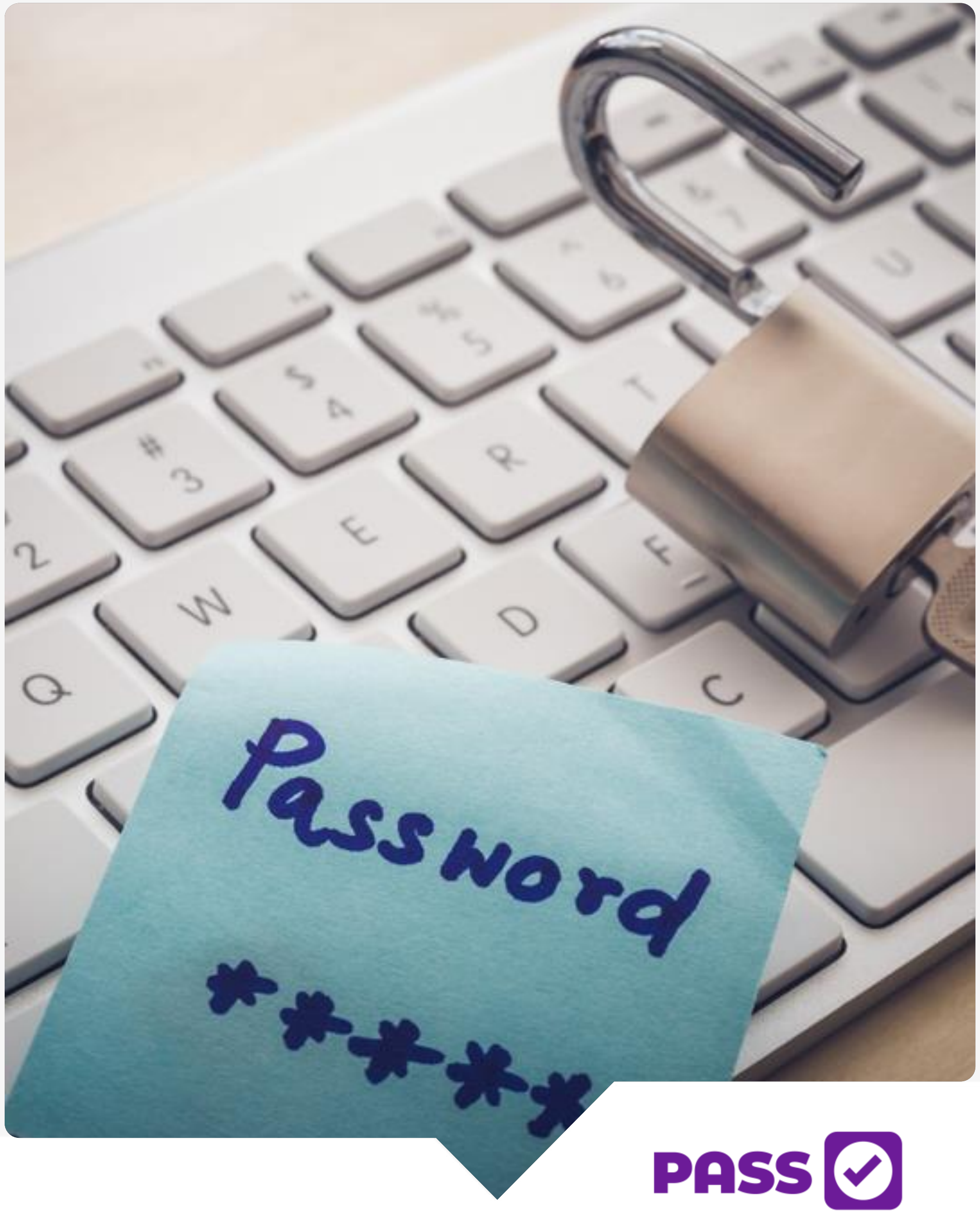


PASS

Data breach

Are the following in place and up to date?

- You have systems in place to effectively manage a data breach. Staff have been trained on how to deal with this situation.
- Your organisation has a data breach process in place whereby all individuals know what to do if a data breach occurs.
- Your organisation has a record management process whereby each breach is logged securely in line with the regulatory requirements.



Continuity & disaster recovery

Can you answer yes to the following?

- You have plans in place for anticipating business disruption and / or disasters that may affect service delivery e.g. 'acts of god', severe weather conditions.
- You have clear processes to follow if you experience an outage for business-critical systems.
- You conduct regular exercises to ensure staff know what to do in the event of unexpected disruption and / or disaster.

PASS

Managing suppliers

Can you confidently evidence

- There needs to be an enforceable supplier contract in place to ensure data protection obligations are met.
- Your organisation's IT system suppliers have the relevant cyber security certification.
- Your organisation has a list of suppliers that handle personal information, the products and services they deliver, and their contact details.
- **TIP:** An external certification such as Cyber Essentials, or ISO27001, or by being listed on Digital marketplace is sufficient.

Transform your care with PASS

Call us on 03300 940 121

PASS