DSPT In depth

DSPT
Better Security.
Better Care.

Digital
Care Hub

Using and Managing Data

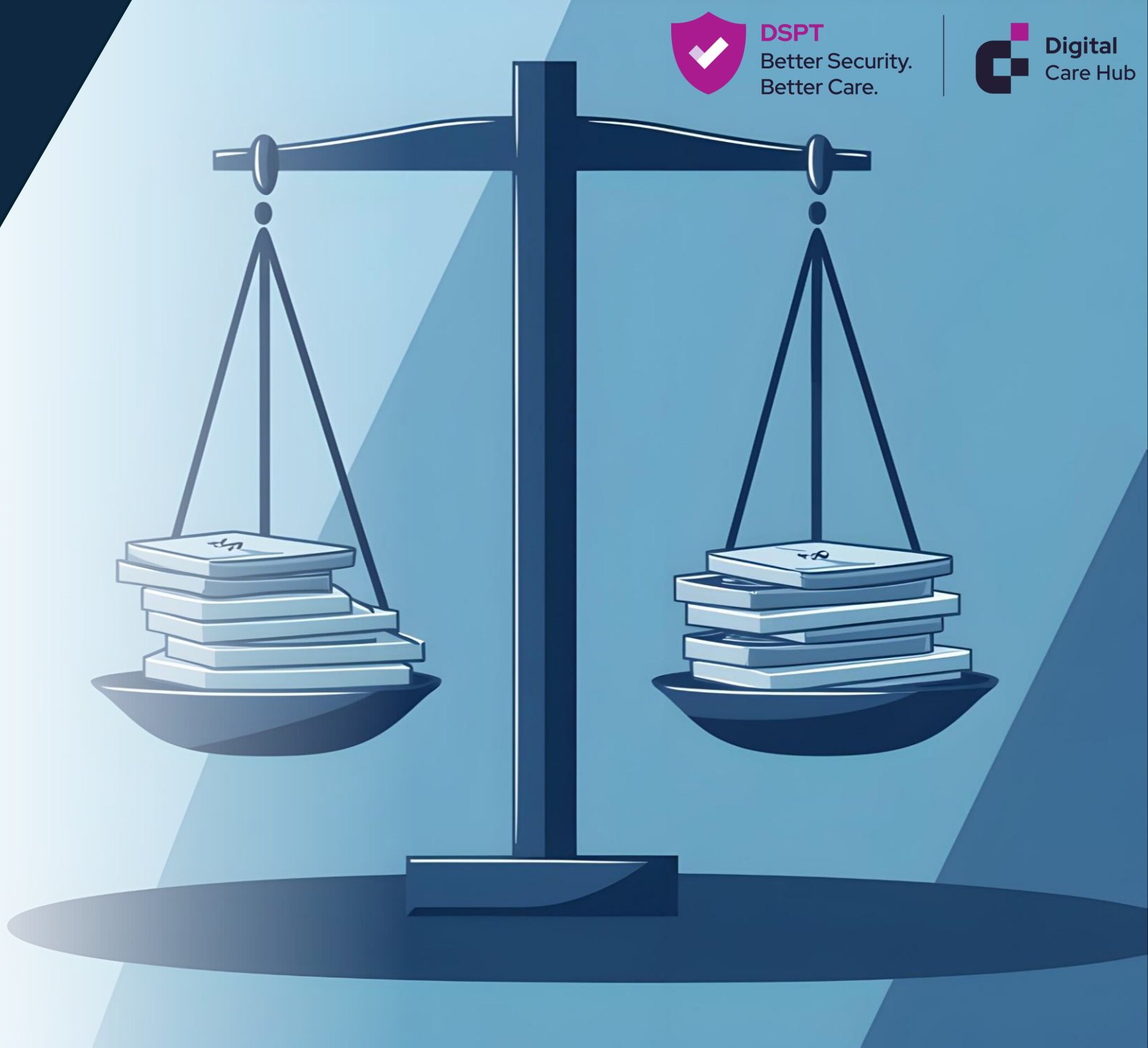
Using and Managing data

- Understand your data
- Policy and data identification
- Staff training/Data controller
- Use and manage the data safely

Legislation

- Data protection legislation controls how your personal information is used by organisations

- The UK data protection is governed by the UK General Data protection Regulation (UK GDPR) and the Data Protection Act 2018



Legislation

Anyone responsible for using personal data must make sure the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- **Accurate** and, where necessary, **kept up to date**
- Kept for **no longer than is necessary**
- Handled in a way that **ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage**

DSPT
Better Security.
Better Care.

Digital
Care Hub

Legislation

- Accurate – Monitoring
- kept up to date – Auditing material
- Kept for no longer than is necessary – Record retention Policy
- Protection against unlawful or unauthorised processing, access, loss, destruction or damage (Data and cyber security controls)

DSPT
Better Security.
Better Care.

Digital
Care Hub

- **Monitor data**: Staffing and roles 1.1.5
- **Kept up to date**: Policies and Procedures 1.1.2
- **Retention of records**: Policies and Procedures 1.4.1
- **Data Protection**: Data security/IT Systems and Devices

Non-compliance consequences

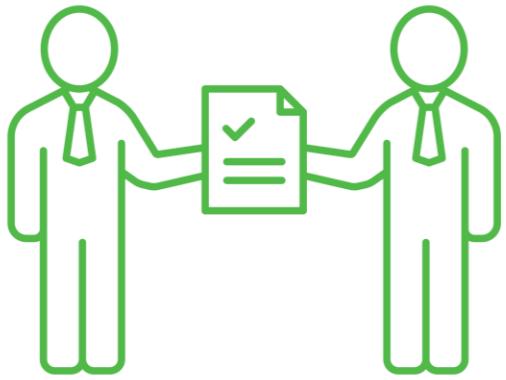
- Detriment to staff, clients, patients, residents, stakeholders
- Reputational damage
- Financial impact
- Time Impact (Business continuity)

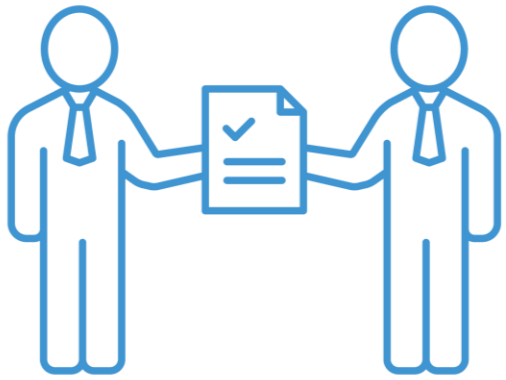
Staff Responsibilities

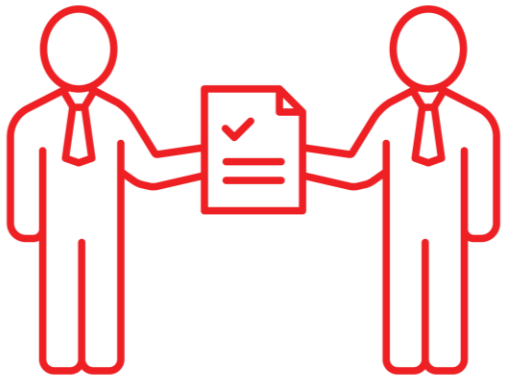
DSPT
Better Security.
Better Care.

Digital
Care Hub

- Everyone is responsible for protecting people's 'personal' and 'confidential' data.
    - Data should only be seen by people who need to see it
    - Data must be complete accurate and up to date
    - Data must be available when it's needed to support care



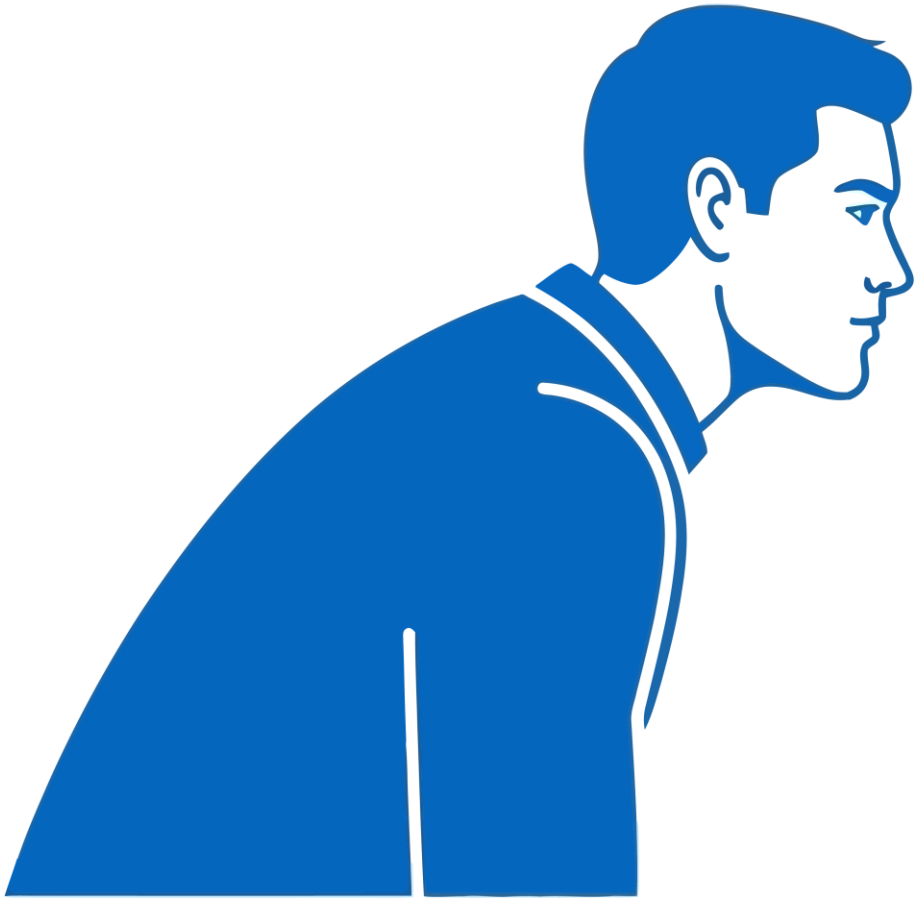


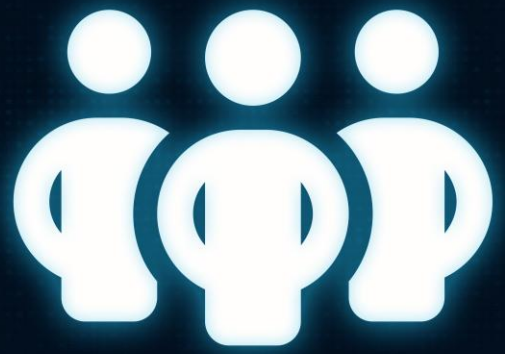


Know your Data

DSPT
Better Security.
Better Care.

Digital
Care Hub





Personal Data

Personal data is defined in the UK GDPR as:

“personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a **name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person**”.

DSPT
Better Security.
Better Care.

Digital
Care Hub

Know your Data – Handling Data

DSPT
Better Security.
Better Care.

Digital
Care Hub

Employer is responsible for putting policies and procedures in place to reduce risks

ROPA, IAR, DPIA

Audit and test

Know your Data

DSPT
Better Security.
Better Care.

Digital
Care Hub

IAR – Information Asset Register

ROPA – Record of Processing Activities

DPIA

Information Asset Register (IAR)

- An Information Asset Register (IAR) is a list of all the places where information is stored, whether the information in that place is special category information, and how that information is kept safe.

DSPT
Better Security.
Better Care.

Digital
Care Hub

Record of Processing Activities (ROPA)

- A Record of Processing Activities (ROPA) is a list of confidential data, where it is received from or where it is sent to and the legal basis for doing this. All data in the IAR marked as being received from or shared with external organisations needs to be included in your ROPA

DSPT
Better Security.
Better Care.

Digital
Care Hub

Data Protection Impact Assessment (DPIA)

- *A DPIA is a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the UK GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations.*

- *It does not have to eradicate all risk, but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.*

DSPT
Better Security.
Better Care.

Digital
Care Hub

- Policies and Procedures: 1.1.2 **(IAR, ROPA)**
- Policies and Procedures: 1.3.8 **(DIPA)**

Roles and Responsibilities Incident Response

- Under GDPR and ICO guidelines certain breaches must be reported within 72hours of incident: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/

DSPT
Better Security.
Better Care.

Digital
Care Hub

Roles and Responsibilities - Incident Response (ICO)

Step 1: Don’t panic

Step 2: Start the timer

Step 3: Find out what’s happened

Step 4: Try to contain the breach

Step 5: Assess the risk

Step 6: If necessary, act to protect those affected

Step 7: Submit your report (if needed)

https://ico.org.uk/for-organisations/advice-for-small-organisations/72-hours-how-to-respond-to-a-personal-data-breach/

Data Protection In Practice

Policies and procedures

Staff training

Personal accountability

Data Protection In Practice

Physical Controls

Auditing

Testing

Spot Checks

Data Protection in Practice

Digital Controls

Building Cyber Resilience

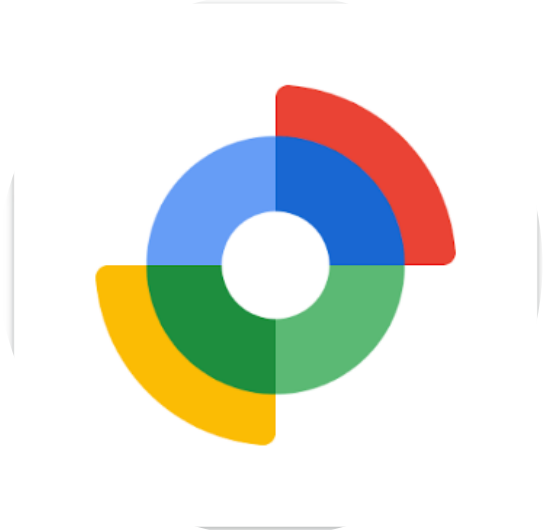
DSPT
Better Security.
Better Care.

Digital
Care Hub

- Develop a strategy for securing networks and devices (DSPT IT systems and devices guidance)
- Bring your own device policy
- Mitigate risk of malware, phishing, hacking
- Cyber resilience staff training
- Secured systems

How to protect your devices

- Switch on screen-lock protection
- Make sure lost and stolen devices can be tracked, locked, or wiped – Google Find my device, Find My IOS
- Keep devices and apps up to date
- Only connect to trusted Wi-Fi networks



DSPT
Better Security.
Better Care.

Digital
Care Hub

Malware Protection

Antivirus - Use reputable antivirus software to detect and remove threats.

MFA and password Policy - Implement policies that require the use of strong, unique passwords for each account..

Education - Human error is a significant risk factor for malware infections.

DSPT
Better Security.
Better Care.

Digital
Care Hub

Passwords

https://www.security.org/how-secure-is-my-password/

DSPT
Better Security.
Better Care.

Digital
Care Hub

MFA (Multifactor authentication)

- The Gateway
- 2 step Verification

DSPT
Better Security.
Better Care.

Digital
Care Hub

Encryption

- Windows BitLocker
- Settings Privacy and security
- IOS, set passcode
- Android, security settings

DSPT
Better Security.
Better Care.

Digital
Care Hub

Records Retention

- https://digital.nhs.uk/data-and-information/information-governance/guidance/records-management-code-of-practice/appendix-ii
- Policy to set out time length in which records are retained. Once they reach this period, they will need to be securely destroyed

Records Retention Why?

- Easier to protect 1 document than it is to protect 2
- If we never remove old records, we must justify and protect
- Too much data, huge IAR, too much time and cost to keep all safe.
- Opens us up to more risk

Destruction of records

DSPT
Better Security.
Better Care.

Digital
Care Hub

- Secure and Safe Destruction
- Physical Data
- Software and Hardware

- Policies and Procedures: 1.4.1 **Retention Schedule**
- Policies and Procedures: 1.4.2 **Third Party Contracts**
- Policies and Procedures: 1.4.3 **Non-Third Party**

Secure Suppliers

- What needs protecting and why?
- Know your Suppliers and Check Their Security
- Understand the Security Risks

DSPT
Better Security.
Better Care.

Digital
Care Hub

Understand the Risks

- What needs protecting and why?
- Know your Suppliers and Check Their Security
- Understand the Security Risks

DSPT
Better Security.
Better Care.

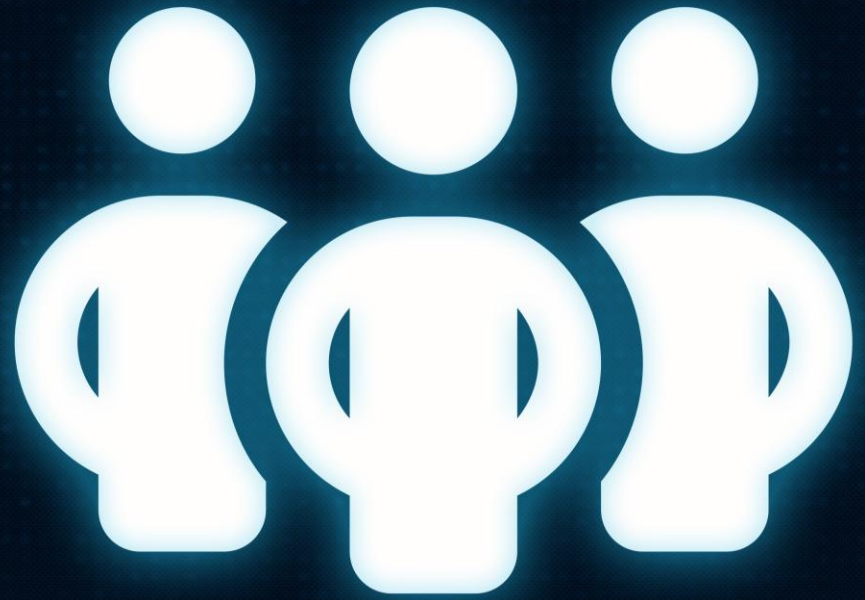
Digital
Care Hub

- Policies and Procedures: 10.1.2 **Supplier List**
- Policies and Procedures: 10.2.1 **Certification**

Business Continuity planning

DSPT
Better Security.
Better Care.

Digital
Care Hub



Why Business Continuity Planning Matters

- Protects vital services for vulnerable people
- Minimises disruption from cyber attacks or system failures
- Demonstrates compliance with laws and regulations

DSPT
Better Security.
Better Care.

Digital
Care Hub

Data protection

- Ensure your data remains protected and recoverable
- Unable to login
- Broken/Lost devices
- System outages/failures
- Cyber attack

DSPT
Better Security.
Better Care.

Digital
Care Hub

Testing and Auditing

- Regularly test recovery processes
- Step 1: Develop a testing schedule
- Step 2: Simulate different scenarios
- Step 3: Document test results
- Step 4: Review and Update Recovery plans

DSPT
Better Security.
Better Care.

Digital
Care Hub

Common pitfalls and how to avoid them

- Lacking correct policy documents
- Misunderstanding around what constitutes Personal Data
- Staff training
- Lack of testing
- Weak or outdated policy
- Lack of policy implementation and auditing
- Treating Data protection as a tick box exercise

Further Support

DSPT
Better Security.
Better Care.

Digital
Care Hub

Digital care hub website: https://www.digitalcarehub.co.uk/

Sussex Digital team: https://www.sussexdigitalteam.co.uk/

My email: sam@sussexdigitalteam.co.uk