

# Data Security and Protection Toolkit (DSPT) Handbook



## The must have guide to the DSPT

This 33-page handbook is an essential tool to support the annual DSPT return

# **Data Security and Protection Toolkit Handbook 2023-2024**

## **Table of contents**

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Guidance statement	2
1.2	Status	2
<b>2</b>	<b>Requirements and support</b>	<b>3</b>
2.1	Rationale	3
2.2	NDG expectations	3
2.3	Care Quality Commission (CQC) expectations	3
<b>3</b>	<b>Data Security Standards</b>	<b>3</b>
3.1	The 10 standards	3
<b>4</b>	<b>Resources</b>	<b>4</b>
4.1	NHS England resources	4
4.2	Organisation lead	4
4.3	Preparing staff	4
4.4	Accessing and registering	5
4.5	Managing users within the DSPT	5
4.6	Managing key roles within the DSPT	5
4.7	Carrying out an assessment	5
4.8	Assertions and evidence	6
4.9	Reporting an incident on the DSPT	6
	<b>Annex A – Mandatory assertion evidence required for 2023-24</b>	<b>8</b>

## 1 Introduction

---

### 1.1 Guidance statement

In England, GP practices are to provide assurance that they have good data security processes in place and patient information is managed appropriately by declaring their compliance with the NHS Digital Data Security and Protection Toolkit (DSPT).

This document will illustrate **[insert organisation name]**'s commitment to the safety of patient information. By adhering to the referenced guidance, staff will ensure that data and information are protected which will reduce the risk of information security incidents in the future.

It is the responsibility of all staff to ensure that they handle patient information and data in the appropriate manner and in accordance with the data security standards.



The following eLearning courses support data protection and can be found in the [HUB](#):

- [Caldicott and Confidentiality](#)
- [GDPR – The Perfect Practice](#)
- [Information Governance and Data Security](#)
- [UK General Data Protection Regulation \(UK GDPR\)](#)

Supporting training guidance on PLUS:

- [Information Governance in the Workplace Induction Training Presentation](#)
- [Information Governance Training Guidance](#)

### 1.2 Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the [Equality Act 2010](#). Consideration has been given to the impact this policy might have regarding the individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment. Furthermore, this document applies to all employees of the organisation and other individuals performing functions in relation to the organisation such as agency workers, locums and contractors.

## 2 Requirements and support

---

### 2.1 Rationale

NHS England's guidance titled [Data Security and Protection Toolkit](#) states that it is an online self-assessment tool that allows organisations to measure their performance against the 10 data security standards of the National Data Guardian (NDG).

This organisation is required to complete an annual assessment to provide assurance that data security is of a good standard and patient information and data are handled in line with the data security standards.

Assessments are to be submitted by 30 June.

### 2.2 NDG expectations

The [NDG standards](#) pertaining to staff are:

- All staff are to ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only to be shared for lawful and appropriate purposes.
- All staff must understand their responsibilities under the NDG data security standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
- All staff are to complete appropriate annual data security training and pass a mandatory test.

### 2.3 Care Quality Commission (CQC) expectations

This handbook should be read in conjunction with the CQC's [GP Mythbuster 85: Data security and protection – expectations for general practice](#).

While the CQC will not directly assess compliance with the [Data Protection Act 2018](#) (including UK GDPR), nor inspect data security, it will want to gain an understanding of how the organisation assures itself that it is effectively protecting patient data.

## 3 Data Security Standards

---

### 3.1 The 10 standards

The purpose of the standards is to enhance existing data security principles, thereby improving data security across the healthcare sector. The standards outline the value of the safe, secure, appropriate and lawful sharing of data.

The [Data Security Standards](#) are:

No	Standard	Supporting guidance
1	<a href="#">Personal confidential data</a>	
2	<a href="#">Staff responsibilities</a>	
3	<a href="#">Staff training</a>	<a href="#">Training needs assessment</a>
4	<a href="#">Managing data access</a>	
5	<a href="#">Process reviews</a>	
6	<a href="#">Responding to incidents</a>	
7	<a href="#">Continuity planning</a>	
8	<a href="#">Unsupported systems</a>	
9	<a href="#">IT protection</a>	
10	<a href="#">Accountable suppliers</a>	

## 4 Resources

---

### 4.1 NHS England resources

NHS England has provided a range of resources to support the introduction of the toolkit and the implementation of the Data Security Standards.

The following are available:

- [About the DSPT](#)
- [DSPT Useful Resources](#)
- [Overview and introductory guidance](#)
- [Frequently asked questions](#)

### 4.2 Organisation lead

At this organisation, there is a nominated lead for the DSPT.

The organisation lead will pinpoint those members of the organisation who require login access to the DSPT to ensure that there is appropriate resilience when completing the annual declaration and when reporting any information governance breaches via the toolkit within the appropriate timescales.

### 4.3 Preparing staff

At this organisation, all staff will be given access to the referenced material to ensure that they understand the requirements associated with the toolkit and are fully aware

of the data security standards outlined in this document and how the standards apply in practical terms.

#### **4.4 Accessing and registering**

To access the DSPT, visit [www.dsptoolkit.nhs.uk](http://www.dsptoolkit.nhs.uk) which is the DSPT homepage.

Select the register button (top right of the screen) to register the organisation. This requires a valid email address and organisation code.

If already registered, then select the 'Log in' button (top right of the screen) and provide an appropriate email address and password.

#### **4.5 Managing users within the DSPT**

Access the [DSPT homepage](#).

Log in with an appropriate email address and password. Click on the 'Admin' tab and select 'Manage Users.'

- To add a 'user,' click the 'Add User' tab, add the email address, select the role (Administrator, Member or Auditor) and click 'Add User'.
- To edit a user's access, select the 'Edit' tab next to the user's name, select role (Administrator, Member or Auditor) or select the 'Remove Access' tab and click 'Save'.

#### **4.6 Managing key roles within the DSPT**

Access the [DSPT homepage](#).

- Log in with an appropriate email address and password
- Click on the 'Organisation' profile tab
- Select the 'Change' tab by the user details that require amendment
- Make the change
- Save

#### **4.7 Carrying out an assessment**

Access the [DSPT homepage](#).

Log in with an appropriate email address and password and click on the 'Assessment' tab.

Previous publications can be reviewed by clicking on the 'View Previous Publications' tab and 'View Details'.

Click on each of the assertions highlighted in blue text.

Entries from the previous year will be auto-populated into the evidence sections. A check will need to be made to ensure that the entries are correct for each assertion.

If not, change the text answer or remove/edit the required document, upload a document, reference an existing uploaded document, specify an intranet or internet link to a document or enter text describing the document's location. Click 'Save'.

Once all mandatory assertions in the category have been completed, as per the evidence guidance in [Section 4.8](#), select the box to confirm that the evidence for the assertion is correct.

When all categories have been completed, the organisation lead will be able to publish the full assessment. It should be noted that once published, the assertions cannot be changed.

## 4.8 Assertions and evidence

Assertions and evidence items are specific to the organisation type. Primary care is classed as a Category 4 organisation. The full list of 2023-24 (version 6) assertions and evidence items can be viewed [here](#).

The spreadsheet offers comprehensive guidance and tips for each assertion and is a useful reference to support staff when completing the assessment. Organisations are to be mindful that some assertions are mandatory and some are not and this may well change from one year to the next. Some assertions may also be added while some are retired.

The full evidence table, coupled with appropriate links to all supporting documents for each assertion, can be found at [Annex A](#).

## 4.9 Reporting an incident on the DSPT

Access the [DSPT homepage](#). Log in with an appropriate email address and password. Click on the 'Report an Incident' tab.

There are three types of breach:

1. **Confidentiality breach** – Unauthorised or accidental disclosure of, or access to, personal data

Confidentiality breach example:

Infection by ransomware (malicious software that encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can later be restored from backup.

However, if a network intrusion still occurred, notification could be required if the incident qualifies as a confidentiality breach (i.e., personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals. Should the attacker not have accessed personal data, the

breach would still represent an availability breach and require notification if there was potential for the rights and freedoms of the individual to be seriously impacted.

2. **Availability breach** – Unauthorised or accidental loss of access to, or destruction of, personal data

Availability breach example:

In the context of a hospital, if critical medical data about patients is unavailable, even temporarily, this could present a risk to individuals' rights and freedoms – for example, operations may be cancelled.

This is to be classified as an availability breach.

3. **Integrity breach** – Unauthorised or accidental alteration of personal data

Integrity breach example:

When a health or social care record has an entry in the wrong record (misfiling) and has the potential to bring about significant consequences, it will be considered an integrity breach. For example, a 'do not resuscitate' notice on the wrong patient's record may result in the significant consequence of death, while an entry recording the patient's blood pressure may not have the same significant result.

Further information on when an incident is reportable under the UK GDPR can be accessed via the following:

- [Guide to the Notification of Data Security and Protection Incidents](#)
- [Information Governance Data Breach Reporting Policy](#)
- [Confidentiality and Data Protection Handbook](#)

The Information Governance Lead, Senior Information Risk Owner (SIRO)/Caldicott Guardian and Data Protection Officer (DPO) must be informed within 24 hours of the incident being identified.

Further to this, the organisation must notify the Information Commissioner's Office (ICO) of any personal data breach within 72 hours. If the breach is likely to result in a high risk to the rights and freedoms of individuals, organisations must also inform those individuals without undue delay.

For urgent security-related incidents that require immediate assistance and support, an organisation is advised to contact the Data Security Centre helpdesk immediately on either:

0300 303 5222 or [enquiries@nhsdigital.nhs.uk](mailto:enquiries@nhsdigital.nhs.uk)

## Annex A – Mandatory assertion evidence required for 2023-24

NOTE: Information in this section has been obtained from [NHS England](https://www.nhs.uk).

### 1. Personal confidential data

All staff ensure that personal confidential data is managed, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

#### ***Assertion 1.1 The organisation has a framework in place to support lawfulness, fairness and transparency***

Evidence reference 1.1.1	What is your ICO registration number?
Type of input	Text
Mandatory	Yes
Evidence required	<p>ICO number</p> <p>Registration with the ICO is a legal requirement for every organisation that uses or shares personal information unless they are exempt as a small charity. If your organisation is not already registered, you should register as a matter of urgency <a href="#">here</a>.</p> <p>You can check whether you are registered and what your ICO registration number is on the <a href="#">ICO website</a>.</p>
Evidence reference 1.1.2	Does your organisation have an up-to-date list of the ways in which it holds and shares different types of personal and sensitive information?
Type of input	Document

Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">Record of Processing Activities</a></li> <li>• <a href="#">Information Asset Register</a></li> </ul> <p>To be compliant with data protection legislation, the organisation must keep a register of all of the information it stores, shares and receives.</p> <p>This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how it is kept safe. The organisation should also have a list or lists of the types of personal data that is shared with others, e.g., needs assessments, prescriptions, pay slips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how the organisation keeps it safe.</p> <p>The register should have been reviewed and approved by the management team at least once in the last twelve months.</p>

Evidence reference 1.1.3	Does your organisation have a privacy notice?
Type of input	Document
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">Practice Privacy Notice</a></li> <li>• <a href="#">Child Privacy Notice</a></li> <li>• <a href="#">Employee Privacy Notice</a></li> <li>• <a href="#">Candidate Privacy Notice</a></li> <li>• <a href="#">Adult Privacy Information Leaflet</a></li> <li>• <a href="#">Children's Privacy Information Leaflet</a></li> </ul>

	<p>If the organisation uses and shares personal data, then it has a duty to tell people what it is doing with it. This includes why the organisation needs the data, what it will do with it, who it is going to share it with and the individual's rights under data protection legislation, e.g., the right to access their information.</p> <p>This needs to be set out in writing in privacy notices. The information should be provided in a clear, open and honest way using language that is easy to read and understand. The privacy notice should cover all data processed, e.g., the data relating to the people the organisation supports and their relatives, staff, volunteers and members of the public.</p>
<b>Evidence reference 1.1.5</b>	<b>Who has responsibility for data security and protection and how has this responsibility been formally assigned?</b>
Type of input	Text
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">Risk Register</a></li> <li>• <a href="#">Caldicott and Confidentiality Policy</a></li> <li>• Information Governance (IG) roles/Responsible Persons Register (within the <a href="#">Access Control Policy</a>)</li> <li>• Senior Information Risk Owner (SIRO)/Senior IG Lead and Caldicott Training Certificates</li> </ul> <p>While data security and data protection are everybody's business, there must be a named person within the organisation who takes overall senior responsibility for data security and protection issues. Their responsibility is to provide senior level leadership and guidance.</p> <p>Provide the name of the person or people within the organisation with overall responsibility for data security and protection along with their roles. Then, for each person, describe how this responsibility has been formally assigned to them. For example, this responsibility could be annotated within their job description or recorded in the minutes of a management meeting and/or by email.</p> <p>There may be additional roles within the organisation such as a Data Protection Officer (DPO) and/or Caldicott Guardian. Should the organisation have an additional specialised roles, guidance can be sought <a href="#">here</a>.</p>

	Further reading about Data Security and Protection Responsibilities can be found <a href="#">here</a> .
--	---

Evidence reference 1.1.6	Your organisation has reviewed how it asks for and records consent to share personal data
Type of input	Yes/No and documents
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">Consent Guidance</a></li> </ul> <p>Generally, consent under data protection law is not appropriate in health and care settings but there are some circumstances when it may be necessary, such as for mailing lists.</p> <p>Consent under the common law duty of confidentiality however is more frequently applicable, e.g., an individual must provide their consent to share information with their carer.</p> <p>The organisation needs to provide details on the processes it uses for gaining this consent.</p> <p>Guidance from the ICO on consent can be sought <a href="#">here</a>.</p>

***Assertion 1.2 Individuals' rights are respected and supported***

Evidence reference 1.2.4	Is your organisation compliant with the National Data Opt-Out policy?
Type of input	Yes/No and documents
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• There is a requirement to be compliant with the <a href="#">national data opt-out guidance</a></li> </ul>

	<p>The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes with some exceptions such as when there is a legal mandate/direction or an overriding public interest, e.g., to help manage the Covid-19 pandemic. As a provider, the organisation should help the people who use its services to understand that they can opt out of their data being used for other purposes. The organisation should check that policies, procedures and privacy notice cover the opt out.</p> <p>From July 2022 it is a legal requirement for all health and social care CQC registered organisations to be compliant with the national data opt out.</p> <p>Further reading can be sought from:</p> <ul style="list-style-type: none"> <li>• NHS Digital <a href="#">Compliance with the national data opt-out</a></li> <li>• Digital Care Hub <a href="#">National Data Opt-Out</a></li> <li>• <a href="#">Confidentiality and Data Protection Handbook</a></li> <li>• <a href="#">Caldicott and Confidentiality Policy</a></li> </ul>
--	--

***Assertion 1.3 Accountability and governance in place for data protection and data security***


Evidence reference 1.3.1	Does your organisation have up to date policies in place for data protection and for data and cyber security?
Type of input	Yes/No and documents
Mandatory	Yes
Evidence required	<p>The organisation should have policies and staff guidance in place communicating the organisation's principles and procedures for data protection. These should be updated every three years at the minimum and a record maintained of when each update was made.</p> <ul style="list-style-type: none"> <li>• <a href="#">Access to Deceased Patients Records Policy</a></li> <li>• <a href="#">Access Control Policy</a></li> </ul>

- [Access to Medical Records Policy](#)
- [Accessible Information Standards Policy](#)
- [Audio-Visual and Photography Policy](#)
- [Cookie Policy](#)
- [Bring Your Own Device Policy](#)
- [Caldicott and Confidentiality Policy](#)
- [CCTV Monitoring Policy](#)
- [Clear Desk and Clear Screen Policy](#)
- [Communication Policy](#)
- [Confidential Waste Policy](#)
- [Confidentiality and Data Protection Handbook](#)
- [Confidentiality Code of Practice](#)
- [Data Quality Policy](#)
- [Data Protection Officer Policy](#)
- [Freedom of Information Policy](#)
- GP2GP Guidance within [Electronic Transfer of and Access to the Healthcare Record](#)
- [IG Incident Breach Reporting Policy](#)
- [Intranet and Social Media Acceptable Use Policy](#)
- [Homeworking Policy and Procedure](#)
- Mobile and Remote Working Agreement (Annex A to [Homeworking Policy and Procedures](#))
- Mobile and Remote Working Risk Assessment (Annex B to [Homeworking Policy and Procedures](#))
- NHS Number Policy within the [Use of NHS Numbers Policy](#)
- [Patient Text Messaging \(SMS\) Policy](#)
- [Portable Device Policy](#)
- Portable Device Assignment Form within the [Portable Device Policy](#)
- [Pseudonymisation and Anonymisation Policy](#)
- [Record Retention Policy](#)
- [Smartcard Policy](#)
- Smartcard Agreement within the [Smartcard Policy](#)
- Social Media Patient Policy within the [Patient Social Medical and Acceptable Use Policy](#)
- Staff IG Declaration Form within the [Staff Monitoring Policy](#)
- [Staff Monitoring Policy](#)

	<ul style="list-style-type: none"> <li>• System administrator requirements and declaration within the <a href="#">Access Control Policy</a></li> <li>• <a href="#">The Governance Handbook</a></li> <li>• Third Party Confidential Agreement (within the <a href="#">Confidentiality and Data Protection Handbook</a>)</li> <li>• <a href="#">Transportation of Confidential Records Policy</a></li> <li>• <a href="#">UK GDPR Policy</a></li> </ul>
--	--

Evidence reference 1.3.2	Does your organisation monitor its own compliance with data protection policies and regularly review the effectiveness of data handling and security controls?
Type of input	Yes/No and documents
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">Confidentiality and Data Protection Handbook</a></li> <li>• Confidentiality Audit Template (Annex G within the <a href="#">Confidentiality and Data Protection Handbook</a>)</li> </ul> <p>The organisation should conduct spot checks to ensure that staff are doing what is in the data protection, staff confidentiality and related policies. These should be undertaken at least every year. Spot checks may be parts of other audits the organisation carries out.</p> <p>The organisation should keep a record that spot checks have been conducted, including details of any actions, who has approved the actions and who is taking them forward, if applicable.</p>

Evidence reference 1.3.6	What are the top three data and cyber security risks in your organisation and how does it plan to reduce those risks?
Type of input	Text
Mandatory	No
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">Risk Register</a></li> </ul>

	<p>All organisations have risks and should be able to identify what they are. Identify the three areas that carry the most risk for the organisation, e.g., cyber-attack, personal data breach.</p> <p>Provide a synopsis of each risk and explain what the organisational plan is to reduce the risk.</p> <p> <a href="#">Risk manager</a> is available as part of the <a href="#">Compliance Package</a> in the <a href="#">HUB</a>.</p>
--	---

Evidence reference 1.3.8	Does your organisation's data protection policy describe how it identifies and minimises risks to personal data when introducing or changing a process or starting a new project involving personal data?
Type of input	Yes/No
Mandatory	No
Evidence required	<ul style="list-style-type: none"> <li>Data Protection Impact Assessment Template (DPIA) (within the <a href="#">UK GDPR Policy</a>).</li> </ul> <p>The policy should describe the process that the organisation has in place to make sure that it systematically identifies and minimises the data protection risks of any new project or plan that involves processing personal data, e.g., when implementing a new clinical record system, installing CCTV, if new remote care or monitoring technology is used, or if there is sharing of data for research or marketing purposes.</p> <p>This type of risk assessment is called a Data Protection Impact Assessment (DPIA). The 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. The DPIA should followed the relevant guidance from the ICO.</p>

Evidence reference 1.3.13	Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data
Type of input	Text

Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• UK GDPR Security Checklist and Risk Assessment Template (Annex E within the <a href="#">Confidentiality and Data Protection Handbook</a>)</li> <li>• <a href="#">Access Control Policy</a></li> <li>• <a href="#">Bring Your Own Device Policy</a></li> <li>• <a href="#">Clear Desk and Clear Screen Policy</a></li> <li>• <a href="#">Smartcard Policy</a></li> </ul> <p>Physical controls that support data protection include lockable doors, windows and cupboards, clear desk procedure, security badges, key coded locks to access secure areas etc.</p> <p>Provide details at high level and, if the organisation uses more than one building, summarise how compliance is assured across the organisation's sites.</p>

***Assertion 1.4 Records are maintained appropriately***

Evidence reference 1.4.1	Does your organisation have a timetable that sets out how long it retains records for?
Type of input	Yes/No and documents
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">Records retention schedule</a></li> </ul> <p>The organisation should have a retention timetable in place for all the different types of records that it holds including finance, staffing and care records. The timetable (or schedule) should be based on the NHS England's <a href="#">Records Management Code of Practice 2023</a>.</p>

Evidence reference 1.4.3	If your organisation destroys any records or equipment that holds personal data, how does it make sure that this is done securely?
Type of input	Text
Mandatory	No
Evidence required	<ul style="list-style-type: none"> <li><a href="#">Confidential Waste Policy</a></li> </ul> <p>It is important when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment such as old computers and laptops, mobile phones, CDs and memory sticks. Briefly describe how the organisation destroys records or equipment securely.</p> <p>If anyone in the organisation destroys any records or equipment themselves, such as shredding documents, briefly describe how the organisation makes sure that this is done securely.</p> <p>If the organisation does not destroy records or equipment or only uses a third party to do so then you can write 'Not Applicable' in the text box.</p>

## 2. Staff responsibilities

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to manage information responsibly and their personal accountability for deliberate or avoidable breaches.

**Assertion 2.1 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards**

Evidence reference 2.1.1	Does your organisation have an induction process that covers data security and protection, and cyber security?
Type of input	Yes/No and documents

Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">IG Induction Guidance</a></li> <li>• <a href="#">IG Training Slides/Information</a></li> </ul> <p>All new staff and volunteers who have access to personal data should have an induction that covers data security and protection as well as cyber security. It is good practice to keep records of who has been inducted and to review the induction process on a regular basis to ensure it is effective and up to date.</p>

***Assertion 2.2 Staff contracts set out responsibilities for data security***

Evidence reference 2.2.1	Do all employment contracts and volunteer agreements contain data security requirements?
Type of input	Yes/No and documents
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">Employment Contract Template</a></li> <li>• <a href="#">Contract of Employment - Employees</a></li> <li>• <a href="#">Contract of Employment - Variable Hours Template</a></li> <li>• <a href="#">Contract of Employment - Ad Hoc or Bank Staff</a></li> <li>• <a href="#">Confidentiality Clause for Employment Contracts</a></li> </ul> <p>Clauses in contracts or agreements should reference data security (confidentiality, integrity and availability). Many contracts commonly focus on just confidentiality.</p> <p>Staff contracts and volunteer agreements should be reviewed to see if they require updating to include a clause on data security.</p>

### 3. Training

All staff complete appropriate annual data security training and pass a mandatory test. Evidence is required.



Information governance eLearning is available in the [HUB](#):

- [Caldicott and Confidentiality](#)
- [GDPR – The Perfect Practice](#)
- [Information Governance and Data Security](#)
- [UK General Data Protection Regulation \(UK GDPR\)](#)

#### **Assertion 3.2 Staff pass the data security and protection mandatory test**

Evidence reference 3.2.1	Have at least 95% of staff completed training on data security and protection and cyber security in the last twelve months?
Type of input	Yes/No and document
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• Copy of organisational training report for <a href="#">IG</a> and <a href="#">UK GDPR</a></li> </ul> <p>All people in the organisation with access to personal data must complete appropriate data security and protection and cyber security training every year. The organisation's training needs analysis should identify the level of training or awareness raising that people need.</p> <p>There is an understanding that due to illness, maternity/paternity leave, attrition or other reasons it may not be possible for 100% of people to receive training every year. Therefore, the target is 95% of people with access to personal data. For clarity, it is the last twelve months prior to the date of publication.</p>

#### 4. Managing data access

Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

***Assertion 4.1 The organisation maintains a current record of staff and their roles***

Evidence reference 4.1.1	Does your organisation have an up-to-date record of people and their roles?
Type of input	Yes/No and document
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>IG Roles/Responsible Persons Register (Appendix C within the <a href="#">Access Control Policy</a>)</li> <li><a href="#">Leaver Exit Checklist</a></li> </ul> <p>The organisation must have a list of all staff and volunteers and their current roles. This list should be kept up to date including any change of role, new starters and removal of leavers. This may be linked to the existing payroll or rostering system.</p>

***Assertion 4.2 The organisation assures good management and maintenance of identity and access control for its networks and information systems***

Evidence reference 4.2.4	Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?
Type of input	Yes/No and documents
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li><a href="#">Access Control Policy</a></li> <li><a href="#">Leaver Exit Checklist</a></li> </ul>

	<p>When people change roles or leave the organisation, there needs to be a reliable way to amend or remove their access to the IT system(s).</p> <p>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 organisational policies and procedures. This includes access to shared email addresses.</p>
--	---

***Assertion 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes***

<b>Evidence reference 4.3.1</b>	<b>Have all the administrators of your organisation's IT system(s) signed an agreement to hold them accountable to higher standards?</b>
Type of input	Yes/No and documents
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">Access Control Policy</a> (includes System Administrator requirements)</li> <li>• System Administrator Declaration Template (Annex D to the <a href="#">Access Control Policy</a>)</li> </ul> <p>The people within the organisation who are IT system administrators may have access to more information than other staff. They therefore need to be held accountable in a formal way to higher standards of confidentiality than others.</p> <p>This requirement also applies to IT system administrators working in external companies who support the organisation's IT systems. This formal agreement could be part of a job description or contract with the IT support company and/or system suppliers.</p>

Evidence reference 4.3.3	Have all staff been notified that their system use could be monitored?
Type of input	Yes/No and documents
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">Employment Contract Template</a></li> <li>• <a href="#">Contract of Employment - Employees</a></li> <li>• <a href="#">Contract of Employment - Variable Hours Template</a></li> <li>• <a href="#">Contract of Employment - Ad Hoc or Bank Staff</a></li> <li>• <a href="#">Confidentiality Clause</a></li> <li>• <a href="#">Smartcard Usage Policy</a></li> <li>• <a href="#">Staff Monitoring Policy</a></li> </ul> <p>Staff are informed and understand that their system use can be monitored and recorded. The notification method is periodic.</p>

***Assertion 4.4 You closely manage privileged user access to networks and information systems supporting the essential service***

Evidence reference 4.4.1	The person with responsibility for IT confirms that IT administrator activities are logged and those logs are only accessible to appropriate personnel
Type of input	Yes/No and documents
Mandatory	No
Evidence required	IT support staff typically have high level access to systems. The activities of these users should be logged and only available to appropriate personnel.

## 5. Process reviews

Processes are reviewed at least annually to identify and improve processes that have caused breaches or near misses or that force staff to use workarounds which compromise data security.

***Assertion 5.1 Process reviews are held at least once per year where data security is put at risk and following data security incidents***

Evidence reference 5.1.1	If your organisation has had a data breach or a near miss in the last year, has the organisation reviewed the process that may have allowed the breach to occur?
Type of input	Yes/No and documents
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• <a href="#">Significant Event and Incident Policy</a></li> <li>• <a href="#">IG Incident Breach Reporting Policy</a></li> <li>• IG Incident Investigation Template (Annex A within the <a href="#">IG Incident Breach Reporting Policy</a>)</li> <li>• IG Incident Register Template (Annex B within the <a href="#">IG Incident Breach Reporting Policy</a>)</li> </ul> <p>The organisation needs to confirm that it has reviewed any processes that have caused a breach or a near miss or that force people to use unauthorised workarounds which could compromise the organisation's data and cyber security. Workarounds could be things such as using unauthorised devices such as home computers or personal memory sticks or forwarding emails to personal email addresses.</p> <p>It is good practice to review processes annually even if a breach or near miss has not taken place.</p> <p>If there have been no breaches or near misses in the last 12 months, then please tick and write 'Not applicable' in the comments box.</p>

***Assertion 5.2 Action is taken to address problem processes as a result of feedback at meetings or in year***

Evidence reference 5.2.1	Are the actions to address problem processes being monitored and assurance given to the management team?
Type of input	Yes/No and documents
Mandatory	No
Evidence required	Explain the governance regarding the escalation of any issues to management through reports and briefing notes during the last 12 months.

## 6. Responding to incidents

Cyberattacks against services are identified and resisted and security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

***Assertion 6.1 A confidential system for reporting data security and protection breaches and near misses is in place and actively used***

Evidence reference 6.1.1	Does your organisation have a system in place to report data breaches?
Type of input	Yes/No and document
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li><a href="#">IG Incident Breach Reporting Policy</a></li> <li>IG Incident Register Template (Annex B within the <a href="#">IG Incident Breach Reporting Policy</a>)</li> <li>IG Incident Investigation Template (Annex A within the <a href="#">IG Incident Breach Reporting Policy</a>)</li> </ul> <p>All staff and volunteers are responsible for noticing and reporting data breaches and it is vital that there is a robust reporting system in the organisation. There is an incident reporting tool within the DSPT which should be used to report health and care incidents to the ICO.</p>

	If a member of staff is not sure whether or not to inform the ICO of a breach, the DSPT incident reporting tool and guide can help them to decide.
--	--

<b>Evidence reference 6.1.2</b>	<b>If your organisation has had a data breach, was the management team notified and did it approve the actions planned to minimise the risk of a recurrence?</b>
Type of input	Yes/No and document
Mandatory	No
Evidence required	<p>In the event of a data breach the management team of the organisation or nominated person should be notified of the breach and any associated action plans or lessons learnt.</p> <p>If no breaches have occurred in the last 12 months, then please tick and write 'Not applicable' in the comments box.</p>

<b>Evidence reference 6.1.3</b>	<b>If your organisation has had a data breach, were all the individuals who were affected informed?</b>
Type of input	Yes/No and document
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>Data Subject Incident Notification Template (Annex C within the <a href="#">IG Breach Reporting Policy</a>)</li> </ul> <p>If your organisation has had a data breach that is likely to result in a high risk of adversely affecting individuals' rights and freedoms, e.g., damage to reputation, financial loss, unfair discrimination or other significant loss, the organisation must inform the individual(s) affected as soon as possible.</p> <p>If your organisation has had no such breaches in the last 12 months, then please tick and write 'Not applicable' in the comments box.</p>

--	--

**Assertion 6.2 All user devices are subject to anti-virus protection while email services benefit from spam filtering and protection deployed at the corporate gateway**

Evidence reference 6.2.1	Do all the computers and other devices used across your organisation have antivirus/anti-malware software which is kept up to date?
Type of input	Yes/No and documents
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• AV/ATP Reports from ICT Provider</li> <li>• Assurance Statement from ICT Provider</li> </ul> <p>This applies to all servers, desktop computers, laptop computers and tablets. Note that antivirus software and anti-malware are the same thing – they both perform the same functions. The organisation may need to ask its IT supplier to assist with answering this question.</p>

**Assertion 6.3 Known vulnerabilities are acted on based on advice from NHS Digital and lessons learned from previous incidents and near-misses**

Evidence reference 6.3.5	Have you had any repeat data security incidents within the organisation during the past 12 months?
Type of input	Text
Mandatory	No
Evidence required	A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones that occurs within three calendar months of a previous occurrence.

	The organisation will need to provide details of the incident(s).
--	---

## 7. Continuity planning

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

***Assertion 7.1 Organisations have a defined, planned and communicated response to data security incidents that impact sensitive information or key operational services***

Evidence reference 7.1.2	Does your organisation have a business continuity plan that covers data and cyber security?
Type of input	Yes/No and document
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li><a href="#">Business Continuity Plan Policy</a></li> </ul> <p>The organisation's business continuity plan should cover data and cyber security, e.g., what would you do to ensure continuity of service if there was a power cut, the phone line/internet went down, the organisation was hacked, a computer broke down or the office became unavailable (e.g., through fire).</p>

***Assertion 7.3 You have the capability to enact your incident response plan including the effective limitation of impact on your essential service. During an incident you have access to timely information on which to base your response decisions***

Evidence reference 7.3.2	All emergency contacts are kept securely in hardcopy and are up to date
Type of input	Yes/No and document
Mandatory	Yes

Evidence required	<ul style="list-style-type: none"> <li>Emergency Contact List <a href="#">Annex B to the Business Continuity Plan</a></li> </ul> <p>Contacts should include phone number as well as email.</p>
-------------------	--

Evidence reference 7.3.4	How does your organisation make sure that there are working backups of all important data and information?
Type of input	Yes/No and document
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>ICT Provider Assurance Statement</li> </ul> <p>It is important to make sure that backups are tested at least annually to ensure data and information can be restored (in the event of equipment breakdown for example).</p> <p>The organisation may need to ask its IT supplier to assist with answering this question.</p>

## 8. Unsupported systems

No unsupported operating systems, software or internet browsers are used within the IT estate.

### ***Assertion 8.3 Supported systems are kept up to date with the latest security patches***

Evidence reference 8.3.1	How do your systems receive updates and how often?
Type of input	Document
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>ICT Provider Assurance Statement</li> </ul>

	This is the organisation's strategy for system updates. The organisation may need to ask its IT supplier to assist with answering this question.
--	--

## 9. IT protection

A strategy is in place to protect IT systems from cyber threats which is based on a proven cybersecurity framework such as Cyber Essentials. This is reviewed at least annually.

### ***Assertion 9.1 All networking components have had their default passwords changed***

Evidence reference 9.1.1	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?
Type of input	Yes/No and document
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>ICT Provider Assurance Statement</li> </ul> <p>Networking components include routers, switches, hubs and firewalls at all of the organisation's locations. The organisation may just have a Wi-Fi routers. This does not apply to the Wi-Fi routers of people working from home.</p> <p>The organisation may need to ask its IT supplier to assist with answering this question.</p>

### ***Assertion 9.2 A penetration test has been scoped and undertaken***

Evidence reference 9.2.1	The annual IT penetration testing is scoped in negotiation between the person with delegated responsibility for data security and the business and testing team including a vulnerability scan
--------------------------	--

	and checking that all networking components have had their default passwords changed to high strength passwords.
Type of input	Yes/No and document
Mandatory	No
Evidence required	<ul style="list-style-type: none"> <li>ICT Provider Assurance Statement</li> </ul> <p>Use the comments field to outline the scope of the organisation's penetration test and redact any elements of the scope that are sensitive.</p> <p>This should be in the last twelve months.</p>

***Assertion 9.3 Systems that handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities***

Evidence reference 9.3.8	The organisation maintains a register of medical devices connected to its network
Type of input	Yes/No and document
Mandatory	No
Evidence required	The register should include vendor/maintenance arrangements and whether network access is given to the supplier/maintainer.

***Assertion 9.5 You securely configure the network and information systems that support the delivery of essential services***

Evidence reference 9.5.2	Are all laptops and tablets or removable devices that hold or allow access to personal data encrypted?
Type of input	Yes/No and document

Mandatory	Yes
Evidence required	<p>Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people). Devices can be further protected, for example, by preventing the use of removable devices like memory sticks. This is called computer port control.</p> <p>The organisation may need to ask its IT supplier to assist with answering this question.</p> <p>If the organisation does not use any mobile devices, or equivalent security arrangements are in place, then tick and write "Not applicable" in the comments box.</p>

## 10. Accountable suppliers

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and for meeting the National Data Guardian's Data Security Standards.

### ***Assertion 10.1 The organisation can name its suppliers, the products and services they deliver and the contract durations***

Evidence reference 10.1.2	Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver and their contact details?
Type of input	Yes/No and document
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>Contracts List or Register Template (Annex F within the <a href="#">Confidentiality and Data Protection Handbook</a>)</li> </ul> <p>The organisation should have a list or lists of the external suppliers that handle personal information such as IT or care planning systems suppliers, IT support, accountancy, DBS checks, HR and payroll services,</p>

	<p>showing the system or services provided.</p> <p>If the organisation has no such suppliers, then 'tick' and write “Not applicable” in the comments box.</p>
--	---

***Assertion 10.2 Basic due diligence has been undertaken against each supplier that handles personal information***

<b>Evidence reference 10.2.1</b>	<b>Do your organisation's IT system suppliers have cyber security certification?</b>
Type of input	Yes/No and document
Mandatory	Yes
Evidence required	<ul style="list-style-type: none"> <li>• ICT Provider Assurance Statement</li> </ul> <p>The 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.</p> <p>An IT systems supplier would include suppliers of systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example.</p>

<b>Evidence reference 10.2.2</b>	<b>Contracts with all third parties that handle personal information are compliant with ICO guidance</b>
Type of input	Yes/No and document
Mandatory	No
Evidence required	A review of all contracts has been undertaken to ensure that they comply with the requirements set out in Article 28 of the UK GDPR.

	If the organisation has no such suppliers, then 'tick' and write “Not applicable” in the comments box.
--	--

**Practice Index Ltd**

4th Floor  
86 - 90 Paul Street  
London  
EC2A 4NE

T: 020 7099 5510

F: 020 7099 5585

E: [info@practiceindex.co.uk](mailto:info@practiceindex.co.uk)

[www.practiceindex.co.uk](http://www.practiceindex.co.uk)



**PRACTICE INDEX**