

Meeting Title	Board of Directors		
Date	21 June 2021	Agenda item	Bo.7.21.19

## Data Security and Protection Toolkit (DSPT) Assessment 2020/21 Final Report

<b>Presented by</b>	Paul Rice, Chief Digital and Information Officer		
<b>Author</b>	Jenny Pope, Head of Information Governance Graeme Holmes, Information Governance Manager		
<b>Lead Director</b>	Paul Rice, Chief Digital and Information Officer		
<b>Purpose of the paper</b>	This paper sets out the recommended Data Security and Protection Toolkit (DSPT) annual assessment update		
<b>Key control</b>			
<b>Action required</b>	For approval		
<b>Previously discussed at/informed by</b>	Information Governance Sub-Committee		
<b>Previously approved at:</b>	<b>Committee/Group</b>	<b>Date</b>	

### Key Options, Issues and Risks

The Data Security and Protection Toolkit (DSPT) is a Department of Health and Social Care (DHSC) policy delivery vehicle that NHS Digital is commissioned to develop and maintain. An online self-assessment tool, it allows organisations to measure their performance and provide an Assurance of Standards Met against all mandatory Assertions in line with the National Data Guardian's data security standards. The 2020/21 DSPT Assessment final submission will take place on or before 30 June 2021.

This paper updates the Board on the final position. It sets out the recommended Data Security and Protection Toolkit (DSPT) annual assessment 'rating'.

There are 42 Assertions (5 are non-mandatory) in total and 110 mandatory evidence items. 38 of Assertions are complete and confirmed at the time of this report. The remaining items are:

**3.4.1 Have your SIRO and Caldicott received appropriate data security and protection training?**  
SIRO training to take place 29 June 2021.

**5.2 Process Reviews**  
Pending Review of Pathology Desk Top Exercise.

The above will be confirmed as complete prior to submission.

### Analysis

Since publication of the 2020/21 Assessment the Information Governance Team has received updates from Assertion Owners and sought assurances from them on the evidence required to comply with the DSPT.

A comprehensive review of all available evidence is ongoing.

Audit Yorkshire has completed a review of a sample of Assertion items this Assessment year. A report of the outcome of the review by Audit Yorkshire is provided as Appendix B and confirms 'Medium' assurance.

It is to be noted that this year, Audit Yorkshire's review was conducted in accordance with the new national DSPT audit framework, Strengthening Assurance, developed for NHS Digital with a new mandated audit

<b>Meeting Title</b>	<b>Board of Directors</b>		
<b>Date</b>	<b>21 June 2021</b>	<b>Agenda item</b>	<b>Bo.7.21.19</b>

approach. This means the format and assurance the report provides is very different to previous years, and the testing was beyond what is asked in the DSPT.

#### **Recommendation**

It is recommended that the Board approves the 2020/21 DSPT Assessment, which equates to a position of compliance with all mandatory Assertion items by 30 June 2021 resulting in a 'Standards Met' position. This is subject to final evidence as outlined above.

<b>Meeting Title</b>	<b>Board of Directors</b>		
<b>Date</b>	<b>21 June 2021</b>	<b>Agenda item</b>	<b>Bo.7.21.19</b>

Risk assessment						
Strategic Objective	Appetite (G)					
	Avoid	Minimal	Cautious	Open	Seek	Mature
To provide outstanding care for patients			g			
To deliver our financial plan and key performance targets			g			
To be in the top 20% of NHS employers			g			
To be a continually learning organisation				g		
To collaborate effectively with local and regional partners					g	
The level of risk against each objective should be indicated. Where more than one option is available the level of risk of each option against each element should be indicated by numbering each option and showing numbers in the boxes.	Low		Moderate	High	Significant	
	Risk (*)					
Explanation of variance from Board of Directors Agreed General risk appetite (G)						

Benchmarking implications (see section 4 for details)	Yes	No	N/A
Is there Model Hospital data relevant to the content of this paper?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Is there any other national benchmarking data relevant to the content of this paper?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Is the Trust an outlier (positive or negative) for any benchmarking data relevant to the content of this paper?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Risk Implications (see section 5 for details)	Yes	No
Corporate Risk register and/or Board Assurance Framework Amendments	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Quality implications	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Resource implications	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Legal/regulatory implications	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Diversity and Inclusion implications	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Performance implications	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Regulation, Legislation and Compliance relevance
<b>NHS Improvement: (please tick those that are relevant)</b>
<input type="checkbox"/> Risk Assessment Framework <input type="checkbox"/> Quality Governance Framework <input type="checkbox"/> Code of Governance <input type="checkbox"/> Annual Reporting Manual
<b>Care Quality Commission Domain:</b> Well Led
<b>Care Quality Commission Fundamental Standard:</b> Good Governance
<b>NHS Improvement Effective Use of Resources:</b> Choose an item.
<b>Other (please state):</b> Data Protection Act 2018, General Data Protection Regulation and Data Security and Protection Toolkit (DSPT) standards

Relevance to other Board of Director's Academy: (please select all that apply)			
People	Quality	Finance & Performance	Other (please state)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

<b>Meeting Title</b>	<b>Board of Directors</b>		
<b>Date</b>	<b>21 June 2021</b>	<b>Agenda item</b>	<b>Bo.7.21.19</b>

## 1 PURPOSE/ AIM

The purpose of this report is to update the Board on the current position of the 2020/21 Data Security and Protection Toolkit (DSPT) Assessment and confirm final approval prior to submission.

## 2 BACKGROUND/CONTEXT

Since publication of the DSPT requirements the Information Governance Team has received updates from Assertion Owners and sought assurances on the evidence they are required to provide to comply with the DSPT. A comprehensive review of all available evidence is nearing completion at the time of this report.

Progress against individual Assertion items is monitored via a separate DSPT plan, a working document previously received by the Information Governance Committee and included as Appendix A.

Audit Yorkshire has completed a two phase review of a sample of Assertion items this Assessment year, Phase 1 in February 2021 concluding Phase 2 in May 2021. A report of the outcome of the review by Audit Yorkshire is included as Appendix B.

## 3 PROPOSAL

Once all mandatory items for a particular Assertion are complete and have been reviewed they are considered 'met'.

Final submission is 30 June 2021 (or before). The national roll out of the DSPT 2020/21 was delayed and published December 2020. The usual submission deadline of 31 March was changed to 30 June for all organisations for this year's assessment due to the pandemic.

A separate 'DSPT plan' tracks progress against each Assertion item, mandatory and non-mandatory, for 2020/21. In addition to the items highlighted on page 1 of this report, any other items marked amber in the DSPT plan require minor or final adjustments prior to submission but are considered evidenced.

The annual internal audit review by Audit Yorkshire has taken place. Phase 1 took place in March and Phase 2 of the audit completed in May 2021. The final Draft report was received 26/05/2021. Any recommendations fundamental to, or supplementing existing evidence, will be completed by the dates shown. If these are necessary for final submission they will be completed by 30 June 2021.

## 4 BENCHMARKING IMPLICATIONS

N/A

<b>Meeting Title</b>	<b>Board of Directors</b>		
<b>Date</b>	<b>21 June 2021</b>	<b>Agenda item</b>	<b>Bo.7.21.19</b>

## 5 RISK ASSESSMENT

Non-compliance with the DSPT could lead to reputational damage to the Trust and scrutiny from external stakeholders. In the event of a serious Information Governance breach, non-compliance with the DSPT may contribute to a decision by the ICO to impose harsh monetary penalties. Risks to the quality of the DSPT Assessment are monitored via the DSPT Plan and via the SIRO.

## 6 RECOMMENDATIONS

The Board is asked to approve the DSPT submission.

## 7 Appendices

Appendix A: DSPT Plan (see separate attachment)

Appendix B: Audit Yorkshire internal audit review report (see separate attachment)

Appendix C: The National Data Guardian 10 data security standards of the DSPT (see below)

NDG Standard	
1 Personal Confidential Data	All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes
2 Staff Responsibilities	All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.
3 Training	All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.
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.
5 Process Reviews	Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
6 Responding to Incidents	Cyber-attacks against services are identified and resisted and CareCERT 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
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
8 Unsupported Systems	No unsupported operating systems, software or internet browsers are used within the IT estate
9 IT Protection	A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually

<b>Meeting Title</b>	<b>Board of Directors</b>		
<b>Date</b>	<b>21 June 2021</b>	<b>Agenda item</b>	<b>Bo.7.21.19</b>

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