

Meeting Title	Board of Directors		
Date	11 May 2023	Agenda item	Bo.5.23.26

## Data Security and Protection Toolkit (DSPT) Assessment 2022/23

Presented by	Paul Rice, Chief Digital and Information Officer		
Author	Jenny Pope, Head of Information Governance Graeme Holmes, Information Governance Manager		
Lead Director	Paul Rice, Chief Digital and Information Officer		
Purpose of the paper	This paper sets out the recommended Data Security and Protection Toolkit (DSPT) 2022/23 annual assessment 'rating'		
Key control			
Action required	For approval		
Previously discussed at/ informed by			
Previously approved at:		Date	
	Digital and Data Transformation Committee	TBC	
Key Options, Issues and Risks			
<p>The Data Security &amp; Protection Toolkit (DSPT) is a Department of Health and Social Care (DHSC) policy delivery vehicle that NHS Digital (now NHSE) is commissioned to develop and maintain. It is an online self-assessment tool that 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 2022/23 DSPT Assessment final submission will take place on 30 June 2023.</p> <p>This paper updates the Board on the expected final position. It sets out the recommended Data Security and Protection Toolkit (DSPT) annual assessment 'rating'.</p> <p>There are 36 Assertions (2 are non-mandatory) in total and 113 mandatory evidence items.</p> <p>29 of the Assertions are complete and 25 confirmed at the time of this report to Board. The accompanying Status Update summarises the items remaining to evidence. These will be confirmed as complete prior to submission.</p>			
Analysis			
<p>During the year the Information Governance Service has sought evidence from the business against the mandatory standards set out in the DSPT, receiving assurance from Assertion Owners that the evidence complies with the DSPT.</p> <p>A review of all available evidence had been completed at the time of this report. A review of remaining evidence is ongoing. Board is asked to note the "Standards Met" rating forecast rating.</p> <p>Audit Yorkshire has completed its review of Assertion items this Assessment year. A draft report of the outcome of the review is with the SIRO. A final version is expected to be available during May.</p>			
Recommendation			
<p>The Board is asked to note the position and delegate approval of the DSPT submission to Digital and Data Transformation Committee/SIRO on behalf of the Board of Directors prior to submission 30th June 2023.</p>			

Meeting Title	Board of Directors		
Date	11 May 2023	Agenda item	Bo.5.23.26

Risk assessment						
Strategic Objective	Appetite (G)					
	Avoid	Minimal	Cautious	Open	Seek	Mature
To provide outstanding care for our patients, delivered with kindness			g			
To deliver our financial plan and key performance targets			g			
To be one of the best NHS employers, prioritising the health and wellbeing of our people and embracing equality, diversity and inclusion					g	
To be a continually learning organisation and recognised as leaders in research, education and innovation				g		
To collaborate effectively with local and regional partners, to reduce health inequalities and achieve shared goals					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 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 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
High Level Risk Register and / or Board Assurance Framework Amendments	<input type="checkbox"/>	<input type="checkbox"/>
Quality implications	<input type="checkbox"/>	<input type="checkbox"/>
Resource implications	<input type="checkbox"/>	<input type="checkbox"/>
Legal/regulatory implications	<input type="checkbox"/>	<input type="checkbox"/>
Equality Diversity and Inclusion implications	<input type="checkbox"/>	<input type="checkbox"/>
Performance Implications	<input type="checkbox"/>	<input type="checkbox"/>

Regulation, Legislation and Compliance relevance
<b>NHS England: (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> Choose an item.
<b>Care Quality Commission Fundamental Standard:</b> Choose an item.
<b>NHS England Effective Use of Resources:</b> Choose an item.
<b>Other (please state):</b>

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

Meeting Title	Board of Directors		
Date	11 May 2023	Agenda item	Bo.5.23.26

## 1 PURPOSE/ AIM

The purpose of this report is to update the Board on the current position of the 2022/23 Data Security and Protection Toolkit (DSPT) Assessment.

It confirms the recommended DSPT annual assessment 'rating' is forecast to be 'Standards Met' against all mandatory items subject to final evidence.

## 2 BACKGROUND/CONTEXT

The Information Governance Service has received updates from Assertion Owners and their assurances on evidence they have provided to comply with the DSPT. A review of available evidence has been completed and is ongoing.

Progress against individual Assertion items is monitored via a separate DSPT plan, a working document. The graph below summarises the position at the time of this report to Board.

Audit Yorkshire has reviewed a sample of Assertion items this Assessment year, A report of the outcome of the review is now in draft. Any recommendations fundamental to, or supplementing existing evidence, will be completed by 30 June 2023 if necessary for final submission.

It is to be noted that Audit Yorkshire's review was conducted in accordance with the new national DSPT audit framework, Strengthening Assurance, developed for NHS Digital (now NHSE) with a new mandated audit approach and introduced in 2020/21. This means the format and assurance the report provides is again very different to previous years, and the testing extends beyond what is asked in the DSPT.

## 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 2023. The previous annual submission deadline of 31 March was changed in 2020/21 for all organisations due to the pandemic.

A separate 'DSPT plan' tracks progress against each Assertion item, mandatory and non-mandatory. Items marked amber in the DSPT plan require minor or final adjustments prior to submission but are considered evidenced.

The SIRO and DDTC reviews the final assessment prior to 30 June 2023 and will be invited to confirm that the DSPT overall self-assessed rating of 'Standards Met' has been achieved.

Meeting Title	Board of Directors		
Date	11 May 2023	Agenda item	Bo.5.23.26



The graph above shows 6 of the Assertion items are incomplete at the time of this report to Board. These are related to Standard NDG 3, 9 and 10. They will be complete prior to the final submission.

NDG 3 - The remaining items relate to mandatory training. At the time of this report the Trust was 87% compliant with all staff IG training against a target of 95% (compliance is taken to be the highest percentage for the period between 1<sup>st</sup> July 2022 to 30<sup>th</sup> June 2023). There is a high level of IG awareness in the Trust but further efforts continue throughout May and June 2023 to raise the compliance level. A reminder will be issued to all staff in May and IG have confirmed Education Services are reminding staff too. A verbal update of the latest position will be provided if requested at the Board meeting.

NDG 9 - The outstanding evidence is the Penetration Test report and scoping.

NDG 10 - Updated suppliers list outstanding

#### 4 BENCHMARKING IMPLICATIONS

N/A

#### 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 an externally reportable serious IG breach, non-compliance with the DSPT may contribute to the Information Commissioner Office (ICO) decision to take any action including potential monetary penalties.

Meeting Title	Board of Directors		
Date	11 May 2023	Agenda item	Bo.5.23.26

Risks to quality of DSPT Assessments are monitored via the DSPT Plan and via the SIRO.

## 6 RECOMMENDATIONS

It is recommended that the Board notes the current position and supports the proposal to delegate approval of the 2022/23 DSPT Assessment prior to 30 June 2023 to the DDTCS/SIRO on the basis of a Standards Met conclusion, which equates to a position of compliance with all mandatory Assertion items by 30 June 2023.

This is subject to final evidence as outlined above.

## 7 Appendices

Appendix A: Summary Position (separate attachment)

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

Appendix C: The National Data Guardian 10 data security standards of the DSPT.

See further [National Data Guardian - GOV.UK \(www.gov.uk\)](https://www.gov.uk/national-data-guardian)

Meeting Title	Board of Directors		
Date	11 May 2023	Agenda item	Bo.5.23.26

## 10 Data Security Standards

Home > Data Protection and Cyber Security > [10 Data Security Standards](#)

In 2017, the Department of Health and Social Care put in policy that all health and social care providers must follow the 10 Data Security Standards. These were developed by the National Data Guardian <https://www.gov.uk/government/organisations/national-data-guardian>

The standards are organised under 3 leadership obligations.

### The 10 Data Security Standards

People	Process	Technology
Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.	Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.	Ensure technology is secure and up to date.
1. 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.	4. 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 data to personal confidential data on IT systems can be attributed to individuals.	8. No unsupported operating systems, software or internet browsers are used within the IT estate.
2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards including their obligation to to handle information responsibly and their personal accountability for deliberate or avoidable breaches.	5. 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.	9. 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.
3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit	6. Cyber attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data <a href="#">breach</a> or a near miss, with a report made to senior management within 12 hours of detection.	10. 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.
	7. 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.	