Bradford Teaching Hospitals
NHS Foundation Trust

Meeting Title	Board of Directors		
Date	27 May 2020	Agenda item	Bo.5.20.18

Data Security and Protection Toolkit (DSPT) Assessment 2019/20 Final Report

Presented by	Cindy Fedell, Chief Digital and Information Officer	
Author	Jenny Pope, Head of Information Governance Graeme Holmes, Information Governance Manager	
Lead Director	Cindy Fedell, Chief Digital and Information Officer	
Purpose of the paper	This paper sets out the recommended Data Security and Protection Toolkit (DSPT) annual assessment 'rating'	
Key control		
Action required	To note	
Previously discussed at/ informed by	Executive and Non-Executive Regulation Committee – 25.3.20	
Previously approved at:	**Committee/Group**	**Date**
	Information Governance Sub-Committee	10 March 2020
	Executive & Non-Executive Regulation Committee	25 March 2020

Key Options, Issues and Risks

The Data Security & Protection Toolkit (DSPT) is a Department of Health and Social Care policy delivery vehicle that NHS Digital is commissioned to develop and maintain. The DSPT is an online self-assessment that allows organisations to measure their performance and provide an assurance against Assertions in line with the National Data Guardian's 10 data security standards. The 2019/20 DSPT Assessment final submission will take place on or before 31 March 2020.

Analysis

During the year the Information Governance (IG) Sub-Committee received regular updates from Assertion owners and reviewed evidence to comply with the DSPT. Status updates were provided to the Quality Committee in the Information Governance report.

A comprehensive review of all available evidence has now been completed by the IG Sub-Committee. A summary of the position is presented in the Appendix. There was one outstanding assertion at the time of the final review - IG Training compliance against a 95% target. The IG Sub-Committee accepted the position as a ''Standards Met' 'rating' pending completion of the training. The IG Sub-Committee discussed the training compliance position and agreed that should compliance not exactly achieve 95% the Quality Committee would be asked to consider, based on evidence provided throughout the year, that the Trust has a high degree of IG awareness and has met the requirement of 95%. As at 16 March 2019 the Trust is currently at 91.85% training compliance. An updated position will be provided to the Quality Committee at its meeting.

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 confirms a 'Significant Assurance' opinion.

The Executive and Non-Executive Regulation Committee approved the DSPT submission on behalf of the Board of Directors.

Recommendation

The Board is asked to note the report and approval from the Executive and Non-Executive Regulation Committee.

Bradford Teaching Hospitals
NHS Foundation Trust

Meeting Title	Board of Directors		
Date	27 May 2020	Agenda item	Bo.5.20.18

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)						

Risk Implications (see section 5 for details)	Yes	No
Corporate Risk register and/or Board Assurance Framework Amendments	☐	☒
Quality implications	☒	☐
Resource implications	☐	☒
Legal/regulatory implications	☒	☐
Diversity and Inclusion implications	☐	☒
Environmental implications	☐	☒

Benchmarking implications (see section 4 for details)	Yes	No	N/A
Is there Model Hospital data relevant to the content of this paper?	☒	☐	☐
Is there any other national benchmarking data relevant to the content of this paper?	☐	☒	☐
Is the Trust an outlier (positive or negative) for any benchmarking data relevant to the content of this paper?	☐	☐	☒

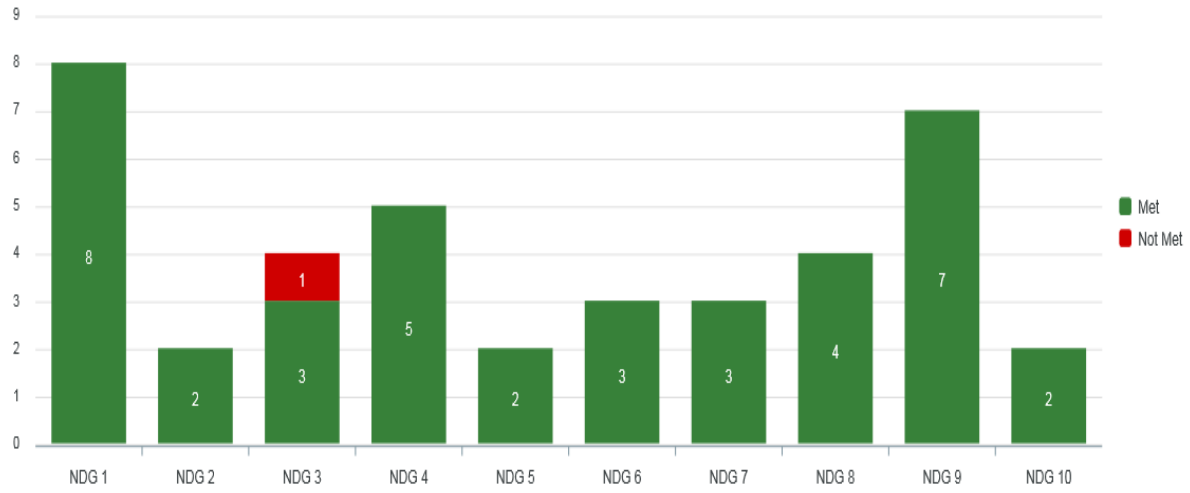
Regulation, Legislation and Compliance relevance
NHS Improvement: (please tick those that are relevant) ☐Risk Assessment Framework ☐Quality Governance Framework ☐Code of Governance ☐Annual Reporting Manual
Care Quality Commission Domain: Well Led
Care Quality Commission Fundamental Standard: Good Governance
NHS Improvement Effective Use of Resources:
Other (please state): Data Protection Act 2018, General Data Protection Regulation and Data Security and Protection Toolkit (DSPT) standards

Relevance to other Board of Director's Committee: (please select all that apply)					
Workforce	Quality	Finance & Performance	Partnerships	Major Projects	Other (please state)
☐	☒	☒	☐	☐	☐

Meeting Title	Board of Directors		
Date	27 May 2020	Agenda item	Bo.5.20.18

Appendix

DSPT Assertion Summary Position as at 10 March 2020



NDG 1 - Personal Confidential Data
NDG 3 - Training
NDG 5 - Process Reviews
NDG 7 - Continuity Planning
NDG 9 - IT Protection
NDG 2 - Staff Responsibilities
NDG 4 - Managing Data Access
NDG 6 - Responding to Incidents
NDG 8 - Unsupported Systems
NDG 10 - Accountable Suppliers

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

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.

Meeting Title	Board of Directors		
Date	27 May 2020	Agenda item	Bo.5.20.18

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
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