

## Appendix A

### Data Security and Protection Toolkit (DSPT) - BTHFT 25/04/2023 Summary Position

36 Assertions (2 are non-mandatory) in total. 105 of 113 mandatory Assertion evidence items have been provided.

The table below summarises the position of all mandatory Assertions. It is split into

- Assertions where some or all its items are 'incomplete' that is, full or partial evidence is still required
- Assertions (entire or items) that the Assertion Owner has provided evidence / a statement against which are ready for IG review. Some may have been reviewed but required further clarity, and
- Assertions (entire or items) that the Assertion Owner has provided evidence / a statement against which have been reviewed by IG.

Once all items for an Assertion are complete and have been reviewed they are considered 'met'. Final submission is 30<sup>th</sup> June 2023.

The table also highlights mandatory Assertion items which are subject to this year's internal audit review by Audit Yorkshire. The completed in March/April 2023. Significant work has been completed to this point; however, some evidence is still outstanding, and reviews cannot take place until it is in place. Assertion Owners have been asked to provide evidence as a matter of priority. Assertions that are subject to audit should ideally be complete. Where not, audit opinion is based on status, taking account of 'plans' for evidencing an Assertion prior to final submission.

Yellow: Subject to audit

	Mandatory Assertions		Notes
Assertion	Description	*Incomplete	
1.1	The organisation has a framework in place to support lawfulness, fairness and transparency	1.1.2 1.1.3	
1.2	Individuals' rights are respected and supported		
1.3	Accountability and Governance in place for data protection and data security		
1.4	Records are maintained appropriately		
2.1	Staff are supported in understanding their obligations under the		

	National Data Guardian's Data Security Standards		
3.1	There has been an assessment of data security and protection training needs across the organisation	3.1.1	Training needs analysis has review date of Feb 2024 though it has been reviewed (June 2021) there were no significant changes to the current document. Agreed with DPO no further review needed this year, though to monitor for any changes which may necessitate further changes. Audit accepted this and state on Audit Report 'Robust procedures for staff data security and awareness induction and ongoing refresher training were found to be in place, underpinned by an appropriate training needs analysis review'
3.2	Staff pass the data security and protection mandatory test	3.2.1	Require organisation training % and turnover / absence rates. Final decision to be agreed prior to submission based on 95% target
3.3	Staff with specialist roles receive data security and protection training suitable to their role	3.3.1 3,3,2	
3.4	Leaders and board members receive suitable data protection and security training	3.4.2	Board Training evidence required
4.1	The organisation maintains a current record of staff and their roles		
4.2	The organisation assures good management and maintenance of identity and access control for its networks and information systems		
4.3	All staff understand that their activities on IT systems will be monitored and recorded for security purposes		
4.4	You closely manage		

	privileged user access to networks and information systems supporting the essential service		
4.5	You ensure your passwords are suitable for the information you are protecting		
5.1	Process reviews are held at least once per year where data security is put at risk and following data security incidents		
6.1	A confidential system for reporting data security and protection breaches and near misses is in place and actively used		
6.2	All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway		
6.3	Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses		
7.1	Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services		

7.2	There is an effective test of the continuity plan and disaster recovery plan for data security incidents	7.2.1 7.2.2	Requires update for in year evidence
7.3	You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions		
8.1	All software and hardware has been surveyed to understand if it is supported and up to date		
8.2	Unsupported software and hardware is categorised and documented, and data security risks are identified and managed	8.2.1, 8.2.2	Assertion owner to update statement. Is Unsupported software list up to date? Has SIRO approved the list and accepted the associated risks?
8.3	Supported systems are kept up to date with the latest security patches		
8.4	You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service		
9.1	All networking components have had their default passwords changed		
9.2	A penetration test has been	9.2.1,9.2.2	Pen Test carried out 21/2/23 Awaiting Pen Test Report and scoping

	scoped and undertaken		document
9.3	Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities	9.3.1	Awaiting Pen Test Report and scoping document
9.4	You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services		
9.5	You securely configure the network and information systems that support the delivery of essential services		
9.6	The organisation is protected by a well managed firewall		
10.1	The organisation can name its suppliers, the products and services they deliver and the contract durations	10.1.1	List being refreshed will be supplied by submission date
10.2	The organisation can name its suppliers, the products and services they deliver and the contract durations	10.2.3	Update required to evidence
Non-Mandatory			
5.2	Participation in reviews is comprehensive, and clinicians are actively involved		
5.3	Action is taken to address problem processes as a result of feedback at meetings or in year		

10.3	All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented		
------	--	--	--