The Queen Elizabeth Hospital King's Lynn
NHS Foundation Trust

Request for Urgent Decision under Standing Order 5 Paragraph 5.2

"5.2 Emergency Powers and urgent decisions

The powers which the Board has reserved to itself within these Standing Orders (see Standing Order 2.7) may in emergency or for an urgent decision be exercised by the Chief Executive and the Chairman after having consulted at least two non-executive members. The exercise of such powers by the Chief Executive and Chairman shall be reported to the next formal meeting of the Trust Board for formal noting. In exercising such powers the Chief Executive and Chairman shall be acting as a committee of the Board."

Title: Data Security Protection Requirements submission to NHSI

Date of request: 24th May 2018 **Authorisation needed by: 25th May 2018**

Request initiated/referred by: M.West / C.Moore

1. Summary: In January 2018, to improve data security and protection for health and care organisations the Department of Health and Social Care, NHS England and NHS Improvement published a set of 10 data and cyber security standards – the 17/18 Data Security Protection Requirements (2017/18 DSPR) – that all providers of health and care must comply with. The 2017/18 DSPR standards are based on those recommended by Dame Fiona Caldicott, the National Data Guardian (NDG) for health and care, and confirmed by government in July 2017. NHSI are asking that all providers confirm whether or not they are complying with the 2017/18 DSPR standards by submitting a web form by 25th May 2018. **As part of the assurance process, the board must sign off our response before it is submitted.** The attached document is a copy of our proposed submission.
2. Policy Implications: Compliance with the DSPR will require changes to existing IT policies and processes, and new ones to be created in order to conform with cyber-related requirements and best practice being communicated by NHS Digital.
3. Financial Implications: It is likely the increased stance in the Trust's posture towards the cyber threat will lead to an increase in costs associated with the more robust IT processes and equipment. The financial risk of not taking the necessary steps potentially outweighs any costs associated with doing so i.e. ICO fine for IT breach.
4. Risk Assessment: Compliance with the DSPR will increase the Trust's stance towards cyber threat, thus helping mitigate the associated risks identified on the Trust's risk register.

5. Reason why matter is urgent NHSI submission is required by COP **25th May 2018**
6. Consultation This document has been agreed and prepared by C.Moore, M.West (ICT) and P.Cottis (IG)
7. Recommendations: Executives are asked to approve the document attached so the same information can be submitted to the NHSI web site by the deadline of the 25th May 2018.

Authorised by:

Chief Executive/ Director	Signature Date -
Chair Edward Libbey – approved by email 23 May 2018	Signature Date – 24 May 2018

To be reported to the Board on 29th May 2018