UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST
BOARD OF DIRECTORS
THURSDAY 26 APRIL 2018

Title:	**APPOINTMENT OF DATA PROTECTION OFFICER**
Responsible Director:	David Burbridge, Director of Corporate Affairs
Contact:	Berit Reglar, Deputy Foundation Secretary, Ext 14324

Purpose:	To ask the Board of Directors to approve the appointment of the Deputy Foundation Secretary as the new Data Protection Officer as required under Article 37 of the General Data Protection Regulation (GDPR). The GDPR will come into force on 25 May 2018.
Confidentiality Level & Reason:	None
Key Issues Summary:	Under Article 37 GDPR, all public bodies and those organisations, where the processing of data forms an inextricable part of their activity ('core activity'), are required to appoint a Data Protection Officer (DPO) who "shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39." Art 39 GDPR, stipulates that the duties of the DPO shall include, but not be limited to, the following tasks: • to inform and advise the controller and the employees who carry out processing of their obligations pursuant to the GDPR and to other data protection provisions; • to monitor compliance with the GDPR, with other data protection provisions and with the Trust's policies, including awareness-raising and training of staff involved in processing operations, and related audits; • to provide advice where requested as regards the data protection impact assessment and monitor their implementation;

	• to cooperate with, and act as the contact point for, the supervisory authority, the Information Commissioner's Office. The DPO needs to report to the highest management level of the organisation, i.e. board level and be able to act independently. The DPO's contact details need to be published on the Trust's website and communicated to the ICO.
Recommendations:	The Board is asked to approve the appointment of the Deputy Foundation Secretary as the Trust's Data Protection Officer.

Approved by:	David Burbridge	**Date:**	16 April 2018

UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST

BOARD OF DIRECTORS

THURSDAY 26 APRIL 2018

USE OF TRUST SEAL

PRESENTED BY DIRECTOR OF CORPORATE AFFAIRS

1. Introduction

1.1. The GDPR introduces a new 'accountability' principle and as such, public bodies and those organisations, where the processing of data forms an inextricable part of their activity ('core activity'), are required to appoint a Data Protection Officer (DPO). The Art 29 Working Party clarified that the 'processing of health data, such as patients' health records, should be considered as one of any hospital's core activities and hospitals must therefore designate DPOs'.

1.2. The DPO will be responsible for many aspects of the GDPR and will therefore need to be chosen carefully in order to ensure that they can meet its demands. The DPO will be required to:

1.2.1. advise the Trust about its obligations when complying with data protection laws

1.2.2. be able to carry out and interpret internal audits against compliance requirements

1.2.3. provide advice on Privacy Impact Assessments and monitor their implementation

1.2.4. be the first point of contact for regulating bodies, authorities and individuals whose data is being used, such as staff and patients

1.2.5. be able to co-ordinate and advise on incident breaches and notification

1.2.6. be familiar with the codes of conduct and risk management

1.2.7. have a good understanding of IT security and associated standards

1.2.8. have excellent communication skills.

1.3. The GDPR does not specify the precise credentials a DPO is expected to have. It does, however, require that they should have professional experience and knowledge of data protection law. Furthermore, the DPO will need to report to to the highest management level of the organisation, i.e. board level and be able to act independently, meaning that they must not receive instructions regarding the exercise of the aforementioned tasks. The DPO cannot be dismissed or penalised for performing their task.

1.4. The DPO may fulfil other tasks and duties, but potential conflicts of interests are to be avoided. The Art 29 Working Party has clarified that 'the DPO cannot hold a position within the organisation that leads him or her to determine the purposes and the means of the processing of personal data. Due to the specific organisational structure in each organisation, this has to be considered case by case. As a rule of thumb, conflicting positions within the organisation may include senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing. In addition, a conflict of interests may also arise, for example, if an external DPO is asked to represent the controller or processor before the Courts in cases involving data protection issues'.

1.5. The DPO's contact details need to be published on the Trust's website and communicated to the ICO.

1.6. Due to the requirement to act independently, undertake a strategic role rather than an operational role, and to report directly to the Board of Directors, it is proposed to appoint the Deputy Foundation Secretary as the Trust's Data Protection Officer.

2. Recommendation

The Board is asked to approve the appointment of the Deputy Foundation Secretary as the Trust's Data Protection Officer.