UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST
BOARD OF DIRECTORS
THURSDAY 27 OCTOBER 2016

Title:	**APPROVAL OF POLICIES**
Responsible Director:	David Burbidge
Contact:	Berit Reglar, Associate Foundation Secretary, Ext 14324

Purpose:	The policies below have been reviewed by all relevant stakeholders and the Policy Review Group and are submitted for approval, as amended.
Confidentiality Level & Reason:	None
Annual Plan Ref:	None
Key Issues Summary:	Save for the IT Acceptable Use Policy, the policies submitted for approval are revised versions which have been updated to take account of changes in legislation and working practices. The IT Acceptable Use Policy is effectively a new policy which seeks to introduce acceptable standards and behaviours in relation to the use of the internet, email, social media websites, mobile devices and IT equipment, whilst maintaining a culture of openness, trust and integrity.
Recommendations:	The Board is asked to consider, and if thought fit, approve: 1. IT Acceptable Use Policy 2. Disciplinary Policy 3. Policy for the development and management of controlled documents

Signed:	David Burbidge	**Date:**	20 October 2016

UNIVERSITY HOSPITALS BIRMINGHAM NHS FOUNDATION TRUST

BOARD OF DIRECTORS
THURSDAY 27 OCTOBER 2016

APPROVAL OF
IT ACCEPTABLE USE POLICY
POLICY FOR SCHEDULING WORKING TIME, and
POLICY FOR THE DEVELOPMENTAND MANAGEMENT OF CONTROLLED DOCUMENTS

PRESENTED BY THE DIRECTOR OF CORPORATE AFFAIRS

1. **IT Acceptable Use Policy**

1.1. The policy sets out the acceptable use, practices and responsibilities expected of Trust staff who are provided with computer, storage, data and media devices to conduct Trust business or interact with internal networks and business systems.

1.2. The policy sets out the expected behaviours of Trust staff when using a variety of electronic media, including:

Email

1.2.1. Trust e-mail accounts must only be used for Trust business, save for, the use of Trust e-mail account for personal purposes, provided this does not interfere with the performance of a member of Trust staff's duties. Personal emails must be marked accordingly in the Subject field.

1.2.2. All e-mails, whether work based or personal, are the property of the Trust, not the member of Trust staff. However, the individual Trust staff member and the Trust will be held jointly liable for communications containing statements about an individual, group or organisation that are proven to be:

- Defamatory
- Blasphemous
- Sexually or racially offensive
- Breach the duty of confidence

1.2.3. Trust staff must not send email in a manner that deliberately attempts to bypass any system log-in or audit functionality or attempt to disguise themselves/their sending address in order to misrepresent any aspect of communication.

Internet

1.2.4. The Trust recognises the benefits of the Internet, and Electronic Communications as valuable business communication tools, which must be used in a responsible, professional and lawful manner and in compliance with the Trust staff code of conduct. The Trust allows the use of these facilities provided patients and staff are protected from any adverse impacts caused by careless or inappropriate usage, confidential information is protected at all times and the Trust's reputation is not put at risk.

Remote/mobile working

1.2.5. Trust staff must ensure that Trust issued equipment will not be left unsecured at any time. Trust staff are further responsible for ensuring that unauthorised individuals are not able to see information or access systems.

1.2.6. Use of any information or devices off-site must be for authorised work purposes only. Authorisation is to be obtained from the Trust staff member's line manager following a risk assessment.

1.2.7. All confidential documentation, whether in paper or electronic format must be stored in a secure area when off-site, and stored securely during transit.

Devices

1.2.8. Non-Trust data devices must not be connected to the Trust network or computers.

Passwords

1.2.9. Passwords and Smartcards must not be shared. Trust staff must not leave any device unattended without activating password protections. Trust staff who discover an unattended device must log out from the session or lock it before commencing their own session.

Software

1.2.10.Downloading personal use applications to Trust mobile devices from the manufacturer's apps store is accepted as long as the application complies with this Policy, and any associated policies and procedures.

1.3. The policy has been developed in conjunction with members of the Information Governance Group and IT services, who will develop associated procedures in support of this policy.

2. Disciplinary Policy

2.1. The policy has been updated as part of the three year review.

2.2. Changes include:

2.2.1. In line with the current and new Policy on Controlled Documents the ‘framework’ section now features before the ‘duties’ section.

2.2.2. The different stages of the disciplinary process have been clarified (e.g. disciplinary hearing as opposed to a disciplinary meeting).

2.2.3. The list of possible gross misconduct has been extended to take account of recent case law.

2.2.4. Further detail has been added to the section dealing with ‘police enquiries’.

2.2.5. A monitoring matrix has been added.

2.2.6. The policy is supported by the Managing Poor Performance Procedure, Disciplinary Procedure and Sickness Absence and Attendance Procedure.

3. Policy for the Development and Management of Controlled Documents

3.1. The Policy has undergone the mandated three year review. As part of this review the Policy has been updated to ensure that it is in accordance with the Human Rights Act 1998 and the Equality Act 2010.

3.2. The Definitions within the Policy have been updated and now include a succinct list of the various types of Controlled Documents used by the Trust. A flow diagram has also been inserted to provide clarity on the difference between clinical and corporate Controlled Documents.

3.3. The Policy sets out clearly that Controlled Documents will remain in force until such time that they are replaced or removed.

3.4. Save for Controlled Documents approved by the chair of the Medicines Management Advisory Group (MMAG) (see Medicines Policy), they must be subject to a stakeholder consultation, led by the Controlled Document Lead, when the Controlled Document is first developed or as part of the 3 yearly review.

3.5. Monitoring of the Policy will ensure all policies adhere to the correct style and format, and that all Controlled Documents have a consultation and ratification process in place.

3.6. The Policy is supported by a detailed Procedure which sets out the requirements for drafting, reviewing/updating, and archiving Controlled

Documents which has also been updated.

4. Recommendation

The Board of Directors are asked to consider, and if thought fit, approve:

4.1. IT Acceptable Use Policy
4.2. Disciplinary Policy
4.3. Policy for the Development and Management of Controlled Documents

David Burbridge
Director of Corporate Affairs
27 October 2016