

**New Starters**  
**Information Governance Checklist**

This procedure must be followed when a member of staff joins the Trust or joins a new department.

**The line manager is responsible for ensuring that each item on this checklist is addressed.**

	<b>ACTION TO BE TAKEN BY LINE MANAGER</b>	✓
1.	Book staff onto mandatory Information Governance training. (See <a href="http://bltintranet/A-Z/InformationGovernance/informationgovernance.aspx">http://bltintranet/A-Z/InformationGovernance/informationgovernance.aspx</a> )	<input type="checkbox"/>
2.	Where the member of staff needs to create or access electronic records, demonstrate the department's shared drive (used for sharing and saving electronic records), how to use the folders and appropriately title documents. (see guidance " <i>Where to store and how to share electronic records</i> " <a href="http://bltintranet/A-Z/Recordsmanagement/guidance.aspx">http://bltintranet/A-Z/Recordsmanagement/guidance.aspx</a> )	<input type="checkbox"/>
3.	Inform staff what they may and may not store on their <b>C</b> and <b>H</b> drives (see guidance " <i>Where to store and how to share electronic records</i> " <a href="http://bltintranet/A-Z/Recordsmanagement/guidance.aspx">http://bltintranet/A-Z/Recordsmanagement/guidance.aspx</a> )	<input type="checkbox"/>
4.	Inform staff that all emails and electronic records created with the Trusts' computers are the property of the Trust, and that emails they write or receive may be released as part of a Freedom of Information request or subject access (Data Protection Act) request.	<input type="checkbox"/>
5.	Where the member of staff may need to share documents with members of their team, explain how to use the shared drive folders rather than send email attachments (see guidance <i>How to Manage Email</i> for more information <a href="http://bltintranet/A-Z/Recordsmanagement/guidance.aspx">http://bltintranet/A-Z/Recordsmanagement/guidance.aspx</a> ).	<input type="checkbox"/>
6.	Inform ICT of the new member of staff and ensure correct contact details been added onto their email profile / properties.	<input type="checkbox"/>
7.	Ensure staff are aware of the appropriate use of email as defined in the Trust's <i>Email Policy</i> .	<input type="checkbox"/>
8.	Instruct staff to regularly delete personal or unimportant emails from their mailbox.	<input type="checkbox"/>
9.	Show staff how to save any important Trust emails onto the relevant paper file or electronic folder.	<input type="checkbox"/>
10.	Inform staff what is appropriate internet use and ensure they are aware that internet access is monitored by ICT.	<input type="checkbox"/>
11.	Show staff how to check their voicemail (where applicable)	
12.	Add member of staff been added to the Trust internal	<input type="checkbox"/>

	phonebook (on the intranet).	
13.	Introduce staff to the department's manual records system (e.g. paper files, microfilm/fiche), and shown how to file, search for and retrieve information.	<input type="checkbox"/>
14.	Where the member of staff has to routinely handle manual records (e.g. lift boxes of files, climb ladders to reach high shelves) book them onto a manual handling training course.	<input type="checkbox"/>
15.	Explain that all Trust records must be retained for a certain period of time in accordance with the Trust records retention & disposal policy, and that any destruction of records should take place in accordance with this policy.	<input type="checkbox"/>
16.	Inform staff how to identify Subject Access Requests / Data Protection requests (requests for personal information) and forward them to the appropriate Trust department for handling.	<input type="checkbox"/>
17.	Inform staff how to identify Freedom of Information (FOI) requests and forward them to the Directorate FOI Lead for handling.	<input type="checkbox"/>
18.	Inform staff that they should report all information security incidents in accordance with the Trust Incident Reporting Policy & Procedure. (e.g. <i>hardware theft, unauthorized access or disclosure, unauthorised loss/destruction of records, etc</i> )	<input type="checkbox"/>
19.	Where the member of staff is handling personal data, inform them who this data may be shared with (internal or external) and what to do if they receive a request for the data from a different source.	<input type="checkbox"/>
20.	Show staff where local confidential waste bins are, for destruction of confidential data.	<input type="checkbox"/>
21.	Inform staff where the local "safe haven faxes" are located and how to use them (see guidance <a href="http://bltintranet/A-Z/InformationGovernance/guidanceandforms/safehavenform.aspx">http://bltintranet/A-Z/InformationGovernance/guidanceandforms/safehavenform.aspx</a> )	<input type="checkbox"/>
22.	Inform staff of appropriate use of the photocopiers and printers, remind them not to leave confidential information there.	<input type="checkbox"/>
23.	Shown how to "lock" the screen when leaving the desk by pressing CTRL, Alt & Delete, to prevent unauthorised access of Trust computers.	<input type="checkbox"/>
	<b>ACTION TO BE TAKEN BY NEW STAFF</b>	
24.	Set up an automatic email signature.	<input type="checkbox"/>
25.	Set up a template out of office message, stating who to contact in case of absence, and including the Trust's standard Freedom of Information message as defined in the Trust Email Policy	<input type="checkbox"/>
26.	Record a new voicemail message (if appropriate).	<input type="checkbox"/>

© Copyright Barts and The London NHS Trust 2006	<b>Author:</b> C Redfern
<b>Version Number:</b> 1.1	<b>Date:</b> 12 February 2007