



### **Essential Information - obtaining a network login and email account**

To access IT systems at the Trust you must agree to abide by the Trust's Acceptable Use Policy. Your manager will request an account on your behalf and supply you with the account details. Your external email address will be in the form `firstname.surname@ldh.nhs.uk`.

If you need access to any other systems in the Trust contact the IT Department to arrange this. For some systems you will be required to attend at least one training session before gaining access to the system. This is due to the complexity of these systems and potential risk to patient care if used incorrectly. You will be given your login to the system after successful completion of the training course.

### **Contacting IT**

This is staffed from 8:30 am to 5:00 pm each weekday, excluding bank holidays. Out of hours emergency support is only available for complete critical patient system failure (PACS, iPM, ICE, etc) and can be contacted via the Trust's switchboard.

### **IT Service Desk**

This provides support for IT issues such as problems with passwords, PCs, email, printers etc. It also provides support for the larger IT systems such as iPM, ICE and PACS.

Telephone: 8666

Email: [ITServiceDesk@ldh.nhs.uk](mailto:ITServiceDesk@ldh.nhs.uk)

### **Training**

Training for the iPM patient database and the ICE clinical ordering system is delivered by the IT Application Support Office. Training can be booked by calling extension 2665. Some training modules can be accessed online when convenient for you. The Application booking assistant will advise you of these.

### **Information and Confidentiality**

IT systems by their very nature give you access to information. You have a duty of care to protect sensitive information, and to keep patient information confidential. Information should only be kept in the relevant IT systems, and should never be kept on a local PC hard drive, PC desktop, or insecure 'shared network drive'. You have a responsibility to ensure that any information you create can only be accessed by staff that have a direct involvement in the use of that information.

### **Acceptable Use**

The Trust has comprehensive policies regarding acceptable use of IT systems, and these form part of your contract of employment. Some essential points for you to note are:

### **Login Accounts**

You will be given login accounts for the IT systems you need to perform your role. These IT systems are auditable - particular actions can be tracked for each login account. You must not share your login with any other member of staff. You will be held responsible for all activity shown under your username.



### **Email and Internet Usage:**

You may not misuse the Trust's email systems. For example, you may not use email or the internet in any way that is likely to be:

- Defamatory, likely to cause offence
- Discriminating, harassing, threatening
- Pornographic, explicit or obscene

You may also not use Hotmail or similar web based free or commercial email systems. The NHS provides a secure web email system for this purpose; contact the IT Department for details.

You may also not use Hotmail or similar web based free or commercial email systems. The NHS provides a secure web email system for this purpose; contact the IT Department for details.

### **Network Usage:**

You may not misuse the Trust's network or systems. A similar list to the above applies. You also may not connect anything other than Trust approved equipment, for example your own personal laptop. PDA devices will need to be encrypted before connection to the Trust's network can be authorised. Call the IT Service Desk where you can speak to someone who will assist in arranging for your PDA to be encrypted (at your own risk) and connected to the network.

### **PC Usage**

You may not misuse the Trust's PCs. This includes installing your own software e.g. Screen savers, which although they can be fun, may also be a primary source of computer viruses and other malware.

This is not an exhaustive list by any means, the Trust's IT and Security Policy is a very comprehensive document and covers these items and many others in much more detail. All of the Trust's policies are available on the Intranet. Please ask your manager to show you where. You are individually responsible for understanding and complying with them.

### **Developing IT to support healthcare**

The IT department is a service organisation. We exist to help you perform your role as effectively as possible. We are committed to developing and implementing IT systems that will improve the way that you work.

If you wish to implement a new IT system of any size, then you must submit a business case to the Trust's Information Systems Steering Group, who will assess your request and how it may be funded. A business case template is available from IT. Please note that IT is not centrally funded, your business case must define how funding will be provided.