

THE NEWCASTLE UPON TYNE HOSPITALS NHS FOUNDATION TRUST

HUMAN RESOURCES SECURITY POLICY

Effective from: Nov 2006

Review Date: Nov 2009

1. Introduction

This document outlines the HR Security Policy in regard to accessing of Newcastle upon Tyne Hospitals NHS Foundation Trust assets and information. Outlining end user and Trust obligations and responsibilities.

2. Security in job definition

- Contracts of employment should include full job descriptions and describe generic duties.
- Where applicable job description should include specific security responsibilities.
- Permanent and contracted staff must sign a statement of confidentiality.
- Terms and conditions should include a statement about the employees responsibility for information security.
- Employee's legal responsibility for information and the responsibility for information security to extend outside the organisation premises.

3. User Training

- The organisation will provide access to training and training materials for all staff on a regular basis.

4. Reporting security Incidents

- All actual or suspected security incidents/breaches must be reported to the ITSO. It is the ITSO responsibility to further report these incidents through the correct channels quickly.

5. Software Malfunctions

- Software malfunctions must be reported via IT help desk
- Users suspecting that a malfunction is due to malicious software should also report to the ITSO.
- Users must not attempt to remove suspect software without authorisation.
- Users must not install unauthorised software. All software loaded onto Trust equipment must be installed by the IT department.
- The Trust will provide and update virus protection software.

5. Disciplinary process

- Users found to be knowingly in breach of information security policy may be subject to disciplinary action.

6. Review

- The Human Resource Manager, in conjunction with the Head of IM&T, is responsible for the review and amendment of this policy.