1 Introduction

The document supports The Newcastle upon Tyne Hospitals NHS Foundation Trust (NuTH) compliance with current statutes and regulations as well as British and International Standards for Software Asset Management (SAM). It lays down the Trust’s policies and procedures in respect of management of its software assets. The means of signifying agreement with these policies and procedures is through the Trust’s Acceptable Use Declaration.

2 Software Asset Management Policy Statement

It is the policy of NuTH to respect all computer software copyrights and adhere to the Terms & Conditions of any licence to which NuTH is a party. The NuTH will not condone the use of any software that does not have a licence and any employee found to be using, or in possession of unlicensed software may be the subject of disciplinary procedures.

It is the responsibility of all NuTH employees, consultants, temporary or contract workers to read, fully understand and signify agreement to The Newcastle upon Tyne Hospitals NHS Foundation Trust’s Acceptable Use Declaration.

The IT Department will maintain all software and related documentation in a central Definitive Media Library (DML) with restricted access.

3 Scope

The policies apply to Newcastle upon Tyne Hospitals NHS Foundation Trust (The Trust) to all people who use or work in the Trust, including employees, honorary contract holders, researchers, trainees, clinical observers and other contractors or individuals involved in patient care and covers e-mail and messaging systems used through Trust computers and servers if these systems are under the jurisdiction and/or ownership of the Trust.

4 Aims

This policy details the legal requirements and user responsibilities for the use of NHS software.
5 Duties (Roles and responsibilities)

It is important that roles and responsibilities are clearly defined and that the scope of ownership of each of the processes is also defined and agreed. The roles and responsibilities are broken down into two distinct groups; Primary and Complimentary.

5.1 Primary Roles

- Management Sponsor– Senior managers within the Trust and IT.
- Director with legal responsibility– Person with the legal responsibility for software assets.
- IT Manager– Responsibility for the configuration management of servers and network infrastructure.
- IT Asset Manager– Responsible for the management of all IT hardware assets within the Trust.
- Software Asset Manager – Responsible for the management of all software assets within the Trust.
- SAM Process Owner– Responsible for the overall effectiveness of the SAM processes.
- Asset Analysts– Responsible for maintaining up-to-date (and historical) records of IT Assets including software version control.

5.2 Complementary Roles

- Security Manager – Helps to ensure that all software is maintained at the recommended security “patch level” so that security exposures are minimised.
- Auditors (Internal/External) – Responsible for reviewing and auditing the SAM processes for efficiency, effectiveness and compliance.
- Procurement Management– Responsible for all aspects of procurement.
- Legal Advice/Counsel – Responsible for all legal advice.
- Change Manager – Responsible for the Change Management process to control all changes with the IT environment including all changes to software.
- Release and Deployment Manager– Controls the release of all software to the live environment.
- Management Tool Analyst– Responsible for the automation of processes where possible.
- Service Desk Manager – First point of contact for user problems and will escalate any discovered unauthorised software to the Software Asset Manager and/or Problem Management.
- SAM Consultant– Provides best practise advice and guidance on aspects of SAM and are external to the Trust.
6 Software Asset Policy

6.1 Software Acquisition

All computer software acquired by the Trust must be purchased by the IT Department through either the Trust’s Strategic Partner or other approved suppliers. No user may purchase software directly and the purchase of software by any other means such as credit cards, expense accounts or petty cash is expressly forbidden. Specialist software for use by the disabled must be accompanied by an assessment from Occupational Health.

All software used within the Trust has been tested to ensure that it meets the requirements of the Trust. All queries/requests for new software must be submitted to the Software Asset Manager via email software.management@nuth.nhs.uk.

6.2 Software Delivery

All newly purchased software will be delivered to the IT Department so that licences can be verified and Asset Registers updated. No other staff may take delivery of computer software.

6.3 Software Installation

Computer software can only be installed by the IT Department; under no circumstances can computer software be installed by any other Trust staff. Non-licensed software and Volume Licensed software will be installed by the IT Service Desk. All other software will be installed by IT as designated to do so by the Software Asset Manager.

6.4 Software Registration

All software will be registered to the Trust and not individual users’ and/or departments irrespective of who purchased the software.

This excludes software that has been supplied on equipment provided by 3rd party organizations such as Universities or companies involved in clinical trials being carried out on Trust properties.

6.5 Software Movements

All staff or department moves must be controlled so that the appropriate software can be added or removed and asset registers updated.

6.6 Software Retirement

The retirement of Software/Hardware used by the Trust may only be carried out by the IT Department.
6.7 Software Disposal

The Disposal of Software/Hardware used by the Trust may only be carried out by the ICT Strategic Partner in compliance with the Waste Electrical and Electronic Equipment (WEEE) Directive.

6.8 Compliance and Documentation

All licences, invoices and original media for all of the software in use in Trust premises are to be held securely by the IT Service Management Office, in particular the Software Asset Manager.

All media must be signed in and out by an authorised person as defined by the Software Asset Manager. A periodic check will be carried out by the IT Service Manager to ensure the actual media matches with the inventory.

6.9 Browser Applications

The Trust has made a business decision that the preferred Browser Application is Internet Explorer (IE) and the current stable version is v7. This is due to a number of Spine Applications which will only work on the IE browser.

If a need exists for another Browser Application then these will be assessed on a need-by-need basis.

6.10 MP3 Programs

Programs such as Apple’s iTunes and the Spotify program are not permitted within the Trust. If there are legitimate business needs for any MP3 programs then these will be assessed on a need-by-need basis.

6.11 Filesharing Programs

Programs that use the BitTorrent format for sharing data are not permitted. This includes, but is not limited to such applications as uTorrent, ABC, BitTorrent Free, etc.

6.12 Fonts

Font software is bound by the same policies and procedures as all software. No user may install any font software onto Trust systems.

6.13 Evaluation (Freeware & Shareware)

Shareware, Freeware & Public Domain software is bound by the same policies and procedures as all software. No user may install any free or evaluation software onto Trust systems.
6.14 Games & Screensavers

The Trust does not permit the use of any screensavers other than those previously agreed. All games are also prohibited on Trust equipment and software policies are in place to disable those games that are supplied as part of the Operating Systems.

6.15 Internet Downloads

No software, whatsoever, must be downloaded from the Internet. To ensure the security of the Trust there are a series of Proxy Servers in place to monitor all Internet traffic and detect all suspect downloads.

6.16 Email Attachments

Users must not load or use any software received via e-mail. Sharing software via email is prohibited.

6.17 Mobile/Laptop Users

Trust software policies apply to mobile users and all laptops will be equipped with auditing software for regular review.

6.18 Disaster Recovery

The owner of every business process and support process is responsible for ensuring that an appropriate business resumption risk assessment is carried out. Where that resumption includes the redeployment or reinstallation of software in support of the business activities the software licensing must comply with this Policy and the conditions of the original Vendor licence.

With regards to Legacy Software it is the responsibility of any department that holds such software hand all copies of the software to the Software Asset Manager for secure storage.

6.19 Disciplinary process

The Trust's software policies are implemented to safeguard the Trust from the many varying laws surrounding software use. Violation of these policies may subject employees or contractors to disciplinary procedures up to and including dismissal.

7 Training

It is the responsibility of all staff to complete the annual mandatory Information Governance training.

8 Equality and diversity

The Trust is committed to ensuring that, as far as is reasonably practicable, the way we provide services to the public and the way we treat our staff reflects their
individual needs and does not discriminate against individuals or groups on any grounds. This document has been appropriately assessed.

9 Auditing and Monitoring

All users must be aware that the Trust electronically audits all computers on a regular basis. A complete internal audit will take place on an annual basis and sample random audits will be performed on a quarterly basis.

<table>
<thead>
<tr>
<th>Standard / process / issue</th>
<th>Monitoring and audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Devices on the Trust network will be monitored on continued basis for software usage with a yearly full audit carried out.</td>
<td>Devices connected to the Trust network will have an Inventory Client installed to monitor software usage and license compliance.</td>
</tr>
<tr>
<td>Further quarterly audits will be carried out with additional ad-hoc audits throughout the year.</td>
<td>Software Asset Manager</td>
</tr>
<tr>
<td></td>
<td>INDIGO Committee</td>
</tr>
<tr>
<td></td>
<td>Continuous process.</td>
</tr>
</tbody>
</table>

10 Consultation and Review

The Software Asset Manager produced this policy which was reviewed and agreed by the Trust Indigo committee.

11 Implementation (including raising awareness)

Technical or regulatory changes to software licenses which may impact on this policy will be implemented through the technical change control process and staff will be advised through IT service management communications.

12 Associated Documentation

- Acceptable Use Declaration
- Disciplinary Procedures
## Policy Title: Software Asset Management Policy

<table>
<thead>
<tr>
<th>1. Does the policy/guidance affect one group less or more favourably than another on the basis of the following: (* denotes protected characteristics under the Equality Act 2010)</th>
<th>Policy Author: Alistair Jack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Race *</td>
<td>No</td>
</tr>
<tr>
<td>Ethnic origins (including gypsies and travellers)</td>
<td>No</td>
</tr>
<tr>
<td>Nationality</td>
<td>No</td>
</tr>
<tr>
<td>Gender *</td>
<td>No</td>
</tr>
<tr>
<td>Culture</td>
<td>No</td>
</tr>
<tr>
<td>Religion or belief *</td>
<td>No</td>
</tr>
<tr>
<td>Sexual orientation including lesbian, gay and bisexual people *</td>
<td>No</td>
</tr>
<tr>
<td>Age *</td>
<td>No</td>
</tr>
<tr>
<td>Disability – learning difficulties, physical disability, sensory impairment and mental health problems *</td>
<td>No</td>
</tr>
<tr>
<td>Gender reassignment *</td>
<td>No</td>
</tr>
<tr>
<td>Marriage and civil partnership *</td>
<td>No</td>
</tr>
</tbody>
</table>

| 2. Is there any evidence that some groups are affected differently? | No |

<table>
<thead>
<tr>
<th>3. If you have identified potential discrimination which can include associative discrimination i.e. direct discrimination against someone because they associate with another person who possesses a protected characteristic, are any exceptions valid, legal and/or justifiable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>4(a). Is the impact of the policy/guidance likely to be negative? (If “yes”, please answer sections 4(b) to 4(d)).</td>
</tr>
<tr>
<td>4(b). If so can the impact be avoided?</td>
</tr>
<tr>
<td>4(c). What alternatives are there to achieving the policy/guidance without the impact?</td>
</tr>
<tr>
<td>4(d). Can we reduce the impact by taking different action?</td>
</tr>
</tbody>
</table>

**Comments:**

- Action Plan due (or Not Applicable):

---

Name and Designation of Person responsible for completion of this form: Alistair Jack. Date: 31/03/2014

Names & Designations of those involved in the impact assessment screening process: INDIGO.

---

For advice on answering the above questions please contact Frances Blackburn, Head of Nursing, Freeman/Walkergate, or, Christine Holland, Senior HR Manager. On completion this form must be forwarded electronically to Steven Stoker, Clinical Effectiveness Manager, (Ext. 24963) steven.stoker@nuth.nhs.uk together with the procedural document. If you have identified a potential discriminatory impact of this procedural document, please ensure that you arrange for a full consultation, with relevant stakeholders, to complete a Full Impact Assessment (Form B) and to develop an Action Plan to avoid/reduce this impact; both Form B and the Action Plan should also be sent electronically to Steven Stoker within six weeks of the completion of this form.