National Institute for Health and Clinical Excellence

Information Technology Policy and Procedures

Responsible Officer	*Ben Bennett, Business Planning & Resources Director*
Author	*Policy Development Group*
Date effective from	*April 2005*
Date last amended	*February 2011*
Review date	*April 2014*

1 Introduction and policy statement

1.1 This document sets out the Information Technology (IT) Policy for NICE for the protection of its IM&T systems and defining baseline responsibilities for IM&T security, equipment and file storage. “IM&T systems” refers to the NICE IT network, hardware including portable media, system and application software, communication components including telephone and WAN systems, documentation, physical environment and other information assets[1]. It does not include IT systems not connected to the NICE IT network.

1.2 This Policy covers the IT networks for NICE staff across all sites and the separate network provided for Evidence & Practice Information Management and Technology in order to manage NICE websites and publishing systems.

1.3 The equipment covered by this policy includes:

- Network Infrastructure – The equipment housed internally to provide the NICE IT network, including servers, enclosures, racks, cabling, switches/hubs, Routers, wireless access points, firewalls, proxies, authentication systems and devices, NTEs, ATAs and remote access systems.
- Desktops – Personal Computers (PCs) issued or provided to staff in the course of carrying out their duties
- Laptops/Netbooks - Portable Personal Computers issued or provided to staff in the course of carrying out their duties
- Mobile Phones/Blackberries - Digital communication devices issued or provided to staff in the course of carrying out their duties
- Desk/Conference Phones – Telephones/Voice Communication devices connected to the Network Infrastructure including desk telephones, conference telephones (star phones), analogue telephony adaptors, DECT telephones (cordless)
- Media/Portable Media – Electronic Storage Devices such as DVDs, CDs, memory sticks and hard drives issued or provided to staff in the course of carrying out their duties
- External Communications Infrastructure – Equipment used to connect NICE to the external world including the Wide Area Network, analogue telephone lines, digital telephone lines, leased lines, LES/WES/Ethernet first mile circuits, ADSL circuits, SDSL circuits and all related equipment and services.
- All related Facilities& Estates controlled IT media used in NICE’s meeting rooms

1.4 The objective of this policy is to ensure: -

- the confidentiality of data and information assets are protected against

[1] An information asset is a definable piece of information, stored in any manner, which is recognised as being 'valuable' to NICE.

unauthorised disclosure and incidents are promptly reported (see section 9)

- the integrity of data and information assets so that they are protected from unauthorised or accidental modification
- the availability and accessibility of IT systems as and when required by staff

1.5 This policy sets out the principles of IT security including the maintenance, storage and disposal of data and explains how they will be implemented at NICE to ensure there is a centralised and consistent approach to IT security.

1.6 One of the aims of the policy aims to raise awareness of the importance of IT security in the day to day business of NICE.

1.7 The policy supports the NICE business objectives of ensuring that the security, integrity and availability of IT systems are balanced against the need for staff to access systems and services that are necessary for their job, within the limits imposed by this policy. It will also help to protect data from misuse and to minimise the impact of service disruption by setting standards and procedures to manage and enforce appropriate IT security.

1.8 The policy supports the legal obligations of NICE to maintain the security and confidentially of its information, notably under the Data Protection Act 1998, the Copyright Patents and Designs Act 1988 and the Computer Misuse Act 1990, and also supports adherence to information governance standards set by the Department of Health (DH).

2 Scope

2.1 This policy applies to all NICE IT systems and those working at or for NICE (Users):

- All NICE employees (including NICE staff on secondment to other organisations)
- Agency workers
- Contractors, where they are directly using NICE's network.
- Secondees (those who are seconded to NICE from other organisations) with authorised access to the IT network.

3 Responsibilities

3.1 Defining responsibilities ensures that all users of NICE IT systems are aware of their responsibilities to minimise the risks to IT security and operations.

3.2 The Business Planning and Resources Director is responsible for ensuring that:

- electronic filing systems and documentation are well maintained for all

critical job functions to ensure continuity;

- no unauthorised staff are allowed to access any NICE IT systems in any location, as such access could compromise data integrity;
- named individuals are given authority to administrate specific computer systems according to their job function and role following the principle of least privilege;
- robust disaster recovery and business continuity procedures are in place;
- all current and new users are instructed in their security responsibilities;
- Procedures are implemented to minimise NICE's exposure to fraud, theft or disruption of its systems; these include segregation of duties, dual control and staff rotation in critical susceptible areas.

3.3 The NICE ICT department has the following responsibilities:

- Day to day responsibility for the management and security of the systems, equipment and services laid out in section 1.3, with specific technical responsibilities being allocated across the team and to outsourced service providers.
- To make all users aware of this policy and to ensure that users understand and are able to abide by them when carrying out work on NICE's behalf.
- Monitoring and reporting on the state of IT security within NICE and across all NICE systems.
- Developing and enforcing detailed procedures to maintain security access to all NICE systems.
- Ensuring compliance with relevant legislation, policies and good practice for all internal systems.
- Monitoring for actual or potential IT security breaches for all internal systems. And reporting to the appropriate people as need be.
- Maintaining an IT asset register (see section 5.1).
- The allocation/disposal/reallocation of all computer hardware and software to ensure best practice usage, value for money and that all data storage devices, including portable electronic media, are purged of sensitive data (such as confidential or personal information) before disposal or reallocation.
- Determining whether or not there is evidence of negligence in use of IT equipment, and reporting any such evidence in accordance with the Incident Reporting procedure.
- Purchasing all computer equipment and software/license to ensure value for money, consistency and compliance.

3.4 NICE Evidence and Practice Directorate IM&T department has the following responsibilities:

- Day to day responsibility for the management and security of the Evidence and Practice IM&T Infrastructure and systems, along with any externally hosted or supplied systems and services. Specific technical responsibilities will be allocated across the IM&T Operations team and

to outsourced service providers.

- To ensure all Users and Systems comply with this policy and further directions that comply with this policy as issued by the CIO for Evidence and Practice from time to time
- Monitoring and reporting on the state of IT security within the NICE IT systems for which they are responsible.
- Providing information on a timely basis to the NICE ICT team to maintain a single asset register for NICE
- Ensuring compliance with relevant legislation.
- Monitoring for actual or potential IT security breaches within the NICE IT systems for which they are responsible. And reporting to the appropriate people as need be.
- Determining whether or not there is evidence of negligence in use of IT equipment, and reporting any such evidence in accordance with the Incident Reporting procedure.
- Ensure any and all information as reasonably required by the Business Planning and Resources Director is provided to fulfil its compliance roles.

3.5 The Human Resources department is responsible for ensuring that:

- all NICE staff sign confidentiality (non-disclosure) undertakings as part of their contract of employment, and any contactors, temporary staff (including agency staff) and secondees sign NICE's standard confidentiality undertaking before they are permitted to use NICE systems.
- the NICE ICT and Evidence and Practice Directorate IM&T department are both notified immediately via the Starters / Leavers / Changers process about changes to user permissions so that access to the IT network can be amended as appropriate. This may include any instance where a member of staff is temporarily suspended from their duties.
- new staff are given basic user training in IT Security as part of their induction.

3.6 Users who **do not** have administration rights over their issued equipment are responsible for ensuring that:

- No breaches of computer security arise or result from their negligence. Users are specifically reminded to keep all passwords and remote log-in data secure (except where necessary to disclose them to the IT department for administrative purposes) and to deny unauthorised third party access to NICE systems. This is particularly important for home workers and when using wireless networks.
- All reasonable care is taken to protect the security of IT equipment they are issued together with confidential data stored on it when taken outside secure offices.
- All reasonable care is taken to protect the security of IT equipment until it is physically returned or declared lost to the NICE IT department regardless of the working state of the equipment.

- Contractors engaged by NICE are provide with and comply with this policy.
- Sensitive data stored on portable IT equipment is kept to the minimum required for business use and encrypted in order to minimise the risks and impacts should a security breach or loss of that equipment occur.
- Actual or suspected security breaches are reported as soon as they arise.
- Only staff explicitly authorised by the NICE ICT dismantle, repair or alter NICE supplied equipment

Further advice is contained in Appendix A.

3.7 Users who **do** have administration rights over their issued equipment are responsibility for ensuring that:

- No breaches of computer security arise or result from their negligence. Users are specifically reminded to keep all passwords and remote log-in data secure (except where necessary to disclose them to the NICE IT or Evidence and Practice Directorate IM&T department for administrative purposes) and to deny unauthorised third party access to NICE systems. This is particularly important for home workers and when using wireless networks.
- All reasonable care is taken to protect the security of IM&T equipment they are issued with together with confidential data stored on it when taken outside secure offices
- All reasonable care is taken to protect the security of IT equipment until it is physically returned or declared lost to the NICE IT department regardless of the working state of the equipment.
- Contractors engaged by NICE are provide with and comply with this policy.
- Sensitive data stored on portable IT equipment is kept to the minimum required for business use and encrypted in order to minimise the risks and impacts should a security breach or loss of that equipment occur.
- Actual or suspected security breaches are reported as soon as they arise.
- Only licensed or in house developed software, specifically required for their job within NICE, is installed upon the equipment for which they are responsible
- The equipment for which they are responsible for is only used for work purposes (no private use) and specifically their own job.
- All due skill, care and attention is taken to ensure that no virus, Trojan spyware or other malware is introduced to their equipment or NICE systems
- All due skill, care and attention is taken to ensure that no configuration, miss-configuration or alteration to systems, software, equipment or infrastructure has a detrimental effect on the normal running, availability or stability of the NICE IT Infrastructure as detailed in section 1.3
- Only staff explicitly authorised by the IM&T Associate Director for Operations dismantle, repair or alter NICE supplied equipment

Further advice is contained in Appendix A.

4 Security

4.1 Technical security measures will be put in place to protect NICE systems from viruses and other malicious software, and all IT systems will be monitored for potential security breaches.

4.2 Contact will be maintained with the appropriate national NHS organisations to ensure that NICE IT systems comply with NHS, Arms Length Body, DH & National standards and best practice regarding IT security management, including N3 connectivity.[2]

4.3 Email and internet use will be governed in accordance with the Email and Internet policy.

4.4 Allocation of accounts to temporary workers using a generic username that cannot be mapped back to the user will not be allowed.

4.5 All relevant contracts with third parties will include standard Office of Government Commerce clauses on information security. All central processing equipment, including file servers, will be covered by third party maintenance agreements.

4.6 All connections to external computer networks and systems including privately owned IT equipment of all kinds must be approved by the NICE IT department and Evidence and Practice Directorate IM&T Operations department.

4.7 All IT equipment, including virtual systems, will be uniquely identified and recorded.

4.8 Environmental controls will be maintained in the server/communications rooms of all premises to protect key equipment. Smoking, drinking and eating is not permitted in these areas.

4.9 Records of all faults and suspected faults will be maintained.

4.10 All NICE laptops must be encrypted with access to NICE IT networks via using a strong authentication method.

4.11 Access to premise server/communications rooms will only be with the express permission of the NICE ICT Department and accompanied by the appropriate representative.

4.12 Memory sticks and other portable media must be encrypted or have password protection when sensitive data is being transported outside secure offices.

5 Software protection

5.1 Only licensed copies of commercial software or in house developed software

[2] N3 Connectivity is the connection between NICE IT systems and the NHS intranet

are used by NICE. The NICE IT department will maintain a register of all commercial software, including all software licenses, to ensure that NICE complies with licence conditions and relevant law. Users must not install ANY externally developed software on NICE IT equipment without prior approval of the IT department or where delegated, the Evidence and Practice Directorate IM&T department

5.2 All users are reminded it is a criminal offence to make or use unauthorised copies of commercial software and that offenders may be liable to disciplinary action.

5.3 Software products required by any department should be approved by the NICE IT Department or Evidence and Practice IMT Operations prior to purchase. Unless otherwise directed all software purchasing and licensing will be carried out by the NICE Procurement department, and users must follow any instructions issued with regard to specific software or applications.

5.4 NICE will minimise the risks of computer viruses through education, good practice and procedures, and application of robust anti-virus software and ensuring firewall policies follow appropriate national guidelines. Users must report any detected or suspected viruses, Trojan, spyware or malware on their computers immediately to the NICE IT Department or Evidence and Practice Directorate IM&T Operations as appropriate.

6 Physical access controls

6.1 Physical access controls to secure areas will minimise the threat to the NICE IT systems through damage or interference. The NICE IT department will be responsible for access to all IT systems located in secure areas, with access being restricted using the principle of least privilege. An entry restriction system to the server/communications rooms at all premises will be implemented.

6.2 The server/communications rooms and store rooms for IT equipment will be locked at all times and the keys/codes held securely by the NICE IT department.

6.3 Authenticated representatives of third party support agencies or other parties will be given access through specific authorisation from the Procurement and IT Manager and will be supervised by NICE IT department representatives while on site.

6.4 No remote access to NICE IT systems will be given to third parties at any time unless specific authorisation is received from the Procurement and IT Manager or the Associate Director of Evidence and Practice IM&T Operations. Such access if granted must be supervised at all times.

7 User access control to the IT network drives

7.1 User access to the IT network drives will be granted where access is necessary to perform the person's job following the principle of least privilege. Access will be modified or removed as appropriate when a person changes job or leaves NICE. It will be the responsibility of the HR department to notify the NICE IT department and the Evidence and Practice Directorate IM&T Operations department immediately of any changes required to access controls, and procedures will be established between the three teams to ensure this happens.

7.2 For those with existing access to the IT network, requests to change access permissions should be made to IT. These will be authorised by the Procurement and IT Manager who will, if necessary, check the requirement with the relevant Director or line manager.

7.3 No individual will be given access to the IT network unless properly trained and made aware of his or her security responsibilities.

7.4 Each member of staff will be provided with a 500 Mb storage space on their 'U drive'. This storage space is free for the individual to use (subject to sections 7.5 & 7.6 below). If this storage limit is exceeded then the U drive will be unable to save any additional data – it is individual's responsibility to manage this allocation.

7.5 'U drives' remain part of the NICE IT systems and NICE has full rights of access to all data stored on its IT network. The content of U drives is not routinely monitored but NICE reserves the right to view content if there are reasonable grounds for doing so; for example to prevent fraud or suspected breach of NICE policies. Further information is contained in the Email and Internet policy.

7.6 Users are not permitted to store entertainment files (including but not limited to music, pictures, video, electronic games) upon the NICE IM&T systems. Files which have the same nature but are for work purposes must be notified to and approved via the NICE IT department

8 Disposal/reallocation of equipment

8.1 Equipment allocated to an individual user (including memory sticks) must not under any circumstances be reallocated within a department (or any other user) and must always be returned to NICE IT for reallocation to ensure correct management of sensitive data

8.2 Where equipment is obsolete for NICE's business purposes but is still in working order and is deemed to be of use to private individuals, that equipment will be offered for sale to NICE staff without any guarantees or warranties. The Finance Department will be notified of any sums due from the buyer of the equipment.

8.3 Where the equipment is deemed to be of no use to private individuals, it will be either disposed of by the Disposal Service Agency (or successor organisation)

or returned to the manufacturer in accordance with the Waste Electrical and Electronic Equipment Directive ("WEEE"). Alternatively it may be passed on to a properly registered charity who will seek to reuse the equipment. As a last resort the equipment will be passed to a properly registered waste carrier for certified recycling.

9 Security incident investigation and reporting

9.1 The objective of security incident investigation is to identify detect, investigate and resolve any suspected or actual computer security breach.

9.2 A security incident is an event that may result in:

- degraded system integrity
- loss of system availability
- disclosure of confidential information
- disruption of activity
- financial loss
- legal action
- unauthorised access to applications
- loss of data

9.3 Incidents should be notified to the Procurement and IT Manager or the Associate Director of Operations (IM&T) as appropriate who will report incidents to the Business Planning and Resources Director and the Audit Committee, in accordance with Incident Reporting Procedure. All security incidents that may have an impact on N3 connectivity will be reported immediately, by the Procurement and IT Manager, to the N3 SP Helpdesk.

9.4 All users must report actual security breaches, or any concerns or suspicions about security breaches, as soon as they arise.

9.5 All actual security incidents will be formally logged, categorised by severity and actions recorded by the NICE IT department, and reported to the Business Planning and Resources Director and the Audit Committee in accordance with Incident Reporting Procedures.

10 Disaster recovery and business continuity

10.1 All business critical data will be replicated between servers at relevant locations so that if the servers in one location become unavailable, access is automatically switched to the servers in another location.

10.2 All data will be backed up onto tape libraries at each site so that data exist in four places (server and tape library at each site). Critical computer equipment must be fitted with battery back-ups (UPS) to ensure that it does not fail during switchovers or emergency shutdowns.

10.3 To minimise the risk to NICE IT systems, robust disaster recovery plans will be

put in place to ensure:

- identification of critical computer systems
- identification of areas of greatest vulnerability and prioritisation of key users and user areas
- agreement with users to identify disaster scenarios and what levels of disaster recovery are required
- development, documentation and testing of disaster recovery plans, including identifying tasks, agreeing responsibilities and defining priorities
- recovery plans cater for different levels of incident, including loss of key user area within a building, loss of building(s), loss of a key part of the IT network, and loss of processing power
- the existence of emergency procedures covering immediate actions to be taken in response to an incident (e.g. alerting disaster recovery personnel) and actions to be taken to return to full normal service

11 Risk management

11.1 The objective of risk management is to identify, counter and report on actual and possible threats to IT systems.

11.2 Significant IT risks will be included in the NICE risk register and will be made available to the Audit Committee.

12 Auditors

12.1 The implementation of NICE's IT policy and procedures will be subject to periodic review by both internal and external auditors and the subsequent recommendations will be agreed and action plans put in place and monitored.

13 Compliance

13.1 Breach of this policy may result in disciplinary action in accordance with the NICE Disciplinary Policy and Procedure. Any breach of the law will be reported to the appropriate authorities.

14 Related Policies

14.1 This policy should be read in conjunction with the following NICE policy and procedure documents:

- E Mail and Internet Policy
- Disciplinary Policy and Procedure Incorporating Suspension Guidelines
- Incident Reporting Procedure
- Data Protection Policy
- Counter Fraud Policy
- Disaster Recovery / Business Continuity Plan
- Risk Management Policy
- Home Working Policy

15 Review

15.1 This policy will be monitored by the IT department to ensure it is fit for purpose and reviewed every 3 years.

16 Signatories

Signed: _____ Date: _____
On behalf of the National Institute for Health and Clinical Excellence

Signed: _____ Date: _____
On behalf of NICE Unison Branch

Signed: _____ Date: _____
On behalf of NICE MiP Branch

Signed: _____ Date: _____
On behalf of NICE Staff Representatives

Appendix A

Good Practice Guide

Below is a summary of recommended Do's and Don'ts for all users of NICE IM&T systems. It is intended to complement approved NICE policies and support new information governance standards set by the Department of Health.

- **Do** ensure you keep security in mind when working – If you have been sent a file or a web link, are you sure you can trust the person it came from, is this the type of thing they would normally send, does it 'feel right'? Remember, lots of spam and viruses sent impersonate the e-mail address of a real person, so the e-mail may not have been sent by the person you think. Lots of viruses move from machine to machine as hidden files on storage devices. Remember, only IT equipment issued, or approved, by the NICE IT department should be used, except where personal PCs and laptops are used in accordance with the Home Working policy.
- **Do** report any errors or problems promptly – If you have an error or an issue, especially if it may be security related, please report it to the IT helpdesk quickly and with as much detail as possible. Reporting that you had a problem 3 days ago and you can't remember the error message makes it almost impossible to track and correct the problem. Reporting promptly with details of which system (e.g. terminal server, e-mail) was affected, the date and time the problem occurred and the specific error message or event makes it much easier to find and fix the problem, and get you working again.
- **Do** think about what you are saving and copying onto the network and in e-mail. Does the file need to be there? How big is it? If you are saving an attachment out of an e-mail, remember to delete the copy in the e-mail to save using up double the space. If you are copying data from a DVD, why is this necessary? If it is only for your use, can it stay on the DVD?
- **Do** take care of the equipment you are issued with, either permanently or on loan. Most of it is expensive and it may contain sensitive or confidential data.
- **Do** remember to return the equipment before leaving NICE. All data will be securely erased by the NICE IT department. Please note that any personal data that has not been erased from returned equipment may be viewed by the IT department.
- **Do** keep passwords secure and never disclose them to anyone else. Passwords should ideally contain at least 9 characters with a mix of letters and symbols in upper and lower case.
- **Do** keep portable media, especially laptops, taken outside NICE offices secure at all times. For example, do not leave them in boots of cars overnight, in overhead luggage racks or unattended in other insecure areas. Where possible carry IT equipment in anonymous cases without a manufacturer's logo and avoid using laptops in public places where possible if confidential information may be visible to other people.

- **Don't** connect any equipment (Laptops, USB devices including storage devices, networking equipment, 3G cards etc.) to NICE IT systems unless it has been supplied or specifically authorised by the NICE IT department. If in any doubt, *confirm* with the helpdesk *before* connecting anything.
- **Don't** download any Software, Software updates, Installation Packages, or Executable files from the Internet or external storage devices (USB sticks, external hard drives, CD-ROM, DVD etc.) onto NICE IT systems unless specifically authorised by the NICE IT Department.
- **Don't** install any software on any NICE IT systems unless specifically authorised by the NICE IT department. All software installs are normally carried out by the NICE IT department and user installation of software is only authorised in special circumstances.
- **Don't** download, upload, store, copy or distribute any materials, data or software of a pornographic, obscene, indecent, racist, defamatory, libellous, sexist, offensive or otherwise unlawful nature (other than for properly authorised and lawful research, for which written notification must be given to the relevant Director).
- **Don't** attempt to circumvent the security and restrictions in place on the NICE IT systems. These are in place to ensure a safe working environment for all staff and maintain the security and resilience of the NICE network.
- **Don't** leave portable media unattended in public places where there is a potential for opportunist theft or compromise (i.e. installation of a virus).
- **Don't** connect any NICE issued equipment or storage devices into another computer or network unless you are happy the network is correctly maintained and up to date Anti-Virus protection is in place. Viruses can be transferred using machines and storage devices connected to compromised computers or networks.
- **Don't** use the NICE network, including U drives, for the storage of music files, as these may breach copyright permissions. Private photographic and or video files should not be stored on U drives as they use up large amounts of space.

For further information and advice please contact the NICE IT department or log a call on the IT Helpdesk.

Appendix B - Version Control Sheet

Version	Date	Author	Replaces	Comment
2	2/2/11	Julian Lewis Barney Wilkinson	IT Policy 2005	