Information Security Policy

Purpose of this document:

This policy is aimed at providing a comprehensive and consistent approach to the security management of information across the Worcestershire NHS community in line with the DH Information Security Management: NHS Code of Practice (April 2007).

The purpose of the policy is to provide a balance between security and ease of use, and to take full account of NHS guidance and legislation.

Key amendments to this Document:

<table>
<thead>
<tr>
<th>Date</th>
<th>Amendment</th>
<th>By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 11</td>
<td>Policy based on CfH template; replacing previous Nov 2007 policy</td>
<td>R King</td>
</tr>
</tbody>
</table>
Contents page:

1. Introduction

2. Objectives, Aim and Scope

   2.1 Objectives
   2.2 Policy Aim
   2.3 Scope

3. Definitions

4. Organisational Responsibilities

   4.1 Chief Executive
   4.2 Director of ICT
   4.3 Senior Information Risk Owner (SIRO)
   4.4 Information Asset Owner (IAO)
   4.5 Information Asset Administrator (IAA)
   4.6 Caldicott Guardian
   4.7 Information Security Officer
   4.8 Information Governance Leads
   4.9 Directors and Departmental Managers
   4.10 System Managers
   4.11 Individual Staff
   4.12 Contractors

5. Legislation

6. Policy Framework

   6.1 Document Framework
   6.2 Information Security Training
   6.3 Contracts of Employment
   6.4 Security Control of Assets
   6.5 Access Controls
   6.6 User Access Controls
   6.7 Computer Access Control
   6.8 Application Access Control
   6.9 Equipment Security
   6.10 Computer and Network Procedures
   6.11 Information Risk Assessment
   6.12 Information Security events and weaknesses
6.13 Classification of Sensitive Information
6.14 Protection from Malicious Software
6.15 User media
6.16 Monitoring System Access and Use
6.17 Accreditation of Information Systems
6.18 System Change Control
6.19 Intellectual Property Rights
6.20 Business Continuity and Disaster Recovery Plans
6.21 Reporting
6.22 Policy Audit
6.23 Further Information

7. Implementation

8. Monitoring and compliance

9. Policy Review

10. References

11. Background

  11.1 Equality requirements
  11.2 Financial Risk Assessment
  11.3 Consultation Process
  11.4 Approval Process

12. Appendices

  Appendix 1 User Responsibility Statement
1. Introduction

This top-level information security policy is a key component of Worcestershire NHS community overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures.

The purpose of this Information Security Policy is to protect, to a consistently high standard, all information assets, including patient records and other NHS corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental. This policy is aimed at providing a comprehensive and consistent approach to the security management of information across the Worcestershire NHS community in line with the DH Information Security Management: NHS Code of Practice (April 2007). It will ensure continuous business capability, and minimise both the likelihood of occurrence and the impacts of any information security incidents.

If any user disregards the rules set out in this Information Security Policy, the user will be fully liable and may be subject to disciplinary action by their employing organisation.

2. Objectives, Aim and Scope

2.1 Objectives

The objectives of Worcestershire Health ICT Services (WHICTS) Information Security Policy are to preserve:

- **Confidentiality** - Access to Data is confined to those who have legitimate authority to view it.
- **Integrity** – Data is timely and accurate and detected or amended only by those specifically authorised to do so.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

2.2 Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by WHICTS:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
• Protecting information assets under the control of the organisation.

2.3 Scope

This policy applies to all full time and part time employees, non-executive directors, contracted third parties (including agency staff), students/trainees and other staff on placement and includes the use of mobile devices.

3 Definitions

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DH</td>
<td>Department of Health</td>
</tr>
<tr>
<td>IAA</td>
<td>Information Asset Administrator</td>
</tr>
<tr>
<td>IAO</td>
<td>Information Asset Owner</td>
</tr>
<tr>
<td>ICT</td>
<td>Information &amp; Communication Technology</td>
</tr>
<tr>
<td>IGT</td>
<td>Information Governance Toolkit</td>
</tr>
<tr>
<td>IG</td>
<td>Information Governance</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>IM&amp;T</td>
<td>Information Management &amp; Technology</td>
</tr>
<tr>
<td>NHS</td>
<td>National Health Service</td>
</tr>
<tr>
<td>NHSCFS</td>
<td>NHS Counter Fraud Services</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PID</td>
<td>Person Identifiable Data</td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority</td>
</tr>
<tr>
<td>SIRO</td>
<td>Senior Information Risk Owner</td>
</tr>
<tr>
<td>SLSP</td>
<td>System Level Security Policies</td>
</tr>
<tr>
<td>WHICTS</td>
<td>Worcestershire Health Information &amp; Communication Technology Services</td>
</tr>
</tbody>
</table>

4 Organisational Responsibilities

4.1 Chief Executive

Information security is the responsibility of all staff within the Worcestershire Trusts. Ultimate responsibility for information security resides with each Trust’s Chief Executive. This responsibility should be discharged through a designated senior member of staff who has lead responsibility.

4.2 Director of ICT

The Director of ICT has been delegated with responsibility for information security on behalf of the Chief Executives’. The day to day activities required to effectively implement and maintain this policy with be performed through the Countywide Information Security Officer.

4.3 SIRO

The Trust’s SIRO (Senior Information Risk Owner) is accountable for fostering a culture for protecting and using data, providing a focal point for managing
information risks and incidents and is concerned with the management of all information assets.

4.4 IAO
The Trust’s IAO’s (Information Asset Owner) role is to understand and address risks to the information assets they ‘own’; and provide assurance to the SIRO on the security and use of these assets.

4.5 IAA
The Trust’s IAA (Information Asset Administrator) will provide support to their IAO by:
- ensuring that policies and procedures are followed, recognising potential or actual security incidents, consulting their IAO on incident management and ensuring that information asset registers are accurate and maintained up to date.

4.6 Caldicott Guardian
The Trust’s Caldicott Guardian has a strategic role in ensuring that there is an integrated approach to information governance, developing security and confidentiality policy and representing confidentiality requirements and issues at Board level.

4.7 Information Security Manager
The Countywide Information Security Manager is responsible for the implementation and enforcement of the Information Security policy. Responsibilities include:

- Ensuring that policies, procedures and working practices align themselves to this information security policy.
- Monitoring and reporting on the status of IT security within the Trusts.
- Ensuring compliance with relevant legislation and regulation.
- Ensuring that staff are aware of their responsibilities and accountability within information security.
- Monitoring for potential security breaches.
- Working closely with those responsible for freedom of information, data protection, patient confidentiality and other information governance work areas.
- Ensuring that risk assessments are carried out along with any associated improvement plans.
- Providing direct input to the information security components of the IG Toolkit.
4.8 Information Governance leads
In addition to the Information Security Officer, each Trust has an information governance lead responsible for:

- Information Governance Management
- Confidentiality and Data Protection
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance.

In addition there exists a County wide Information Governance Group which comprises the Information Governance leads and the Information Security Officer. Through this group common approaches are agreed to aspects of Information Governance where appropriate. Together they have joint responsibility for completion of the IG Toolkit.

4.9 Directors and departmental managers
Directors and departmental managers must ensure:

- They are kept appraised of all information security and governance guidance
- That all staff are aware of their security responsibilities
- That staff have appropriate training for the systems they are using
- That appropriate levels of access are granted to specific individuals (e.g. Registration Authority role for staff who issue smartcards)
- Ensure that all staff sign confidentiality agreements as part of their contract of employment
- Ensure that RA and system managers are informed of staff role changes, new starters and leavers.
- The security of physical environments where information is processed or stored

4.10 System Managers
A system manager will be designated for each information system within the Trust and will be responsible for the day to day management of that system, including a system specific Information Security Policy. The system manager will ensure that the Information Security Policy and associated procedures are enforced within their local area.
4.11 Individual staff

All staff, including contract and temporary workers are:

- Responsible for conformance to the information security policy and associated guidelines and best practice.
- Expected to report information security incidents to their line manager in accordance with local incident reporting procedures.
- Required to sign a general statement of confidentiality on commencement of employment.

Required to sign the User Responsibility Statement that is contained within the Information Security Declaration (Appendix 1 of this document). This is as an indication that they accept responsibility for maintaining security and confidentiality and that they understand the consequences of any breach.

4.12 Contractors

In addition to the responsibilities for individual staff, as detailed above, the contractor must obtain authorisation for use of their laptop on trust premises. This should be obtained through the Trust’s manager they are reporting to who will co-ordinate the request with WHICTS. Any requirement to store Trust’s data on the laptop must have been specifically authorised by the Trust’s manager, and where appropriate, if Person Identifiable Data (PID), confidential or sensitive information the Caldicott Guardian/Information Governance Manager/Information Asset Owner (IAO)/Senior Information Risk Owner (SIRO); Information Governance will be able to clarify this process further details can be found on the Connecting for Health Website. The laptop needs to be encrypted to the approved level; this can be verified with WHICTS.

5. Legislation

The Worcestershire NHS community is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Worcestershire NHS community, who may be held personally accountable for any breaches of information security for which they may be held responsible, failure to comply could result in the individual or the Trust being prosecuted. The Worcestershire NHS community shall comply with the legislation, detailed in section 10, and other legislation as appropriate:
6. Policy Framework

6.1 Document Framework

<table>
<thead>
<tr>
<th>Document Title</th>
<th>Content</th>
<th>Review period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Policy</td>
<td>Principles</td>
<td>2 Years</td>
</tr>
<tr>
<td>User Responsibility Declaration</td>
<td>Statement</td>
<td>2 Years</td>
</tr>
<tr>
<td>Information Security Policies</td>
<td>Requirements</td>
<td>2 Years</td>
</tr>
<tr>
<td>• Access Control Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Anti-Virus Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Back-Up Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Business Continuity Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Equipment Disposal Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Home working Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Internet and E-Mail Access Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mobile Devices Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Network Security Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Safe Haven Policy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6.2 Information Security Awareness Training

- Information security awareness training shall be included in the staff induction process.
- An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

6.3 Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

6.4 Security Control of Assets

Each IT asset, (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.
6.5 Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data.

6.6 User Access Controls

Access to information shall be restricted to authorised users who have a bona-fide business need to access the information.

6.7 Computer Access Control

Access to computer facilities shall be restricted to authorised users who have business need to use the facilities.

6.8 Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

6.9 Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. This will be achieved by the effective use of suitable security measures i.e. physical controls within buildings, entry systems and secure storage facilities to protect assets from theft/damage.

6.10 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by WHICTS.

6.11 Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of Worcestershire NHS community risk management programme. These reviews shall help identify...
areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

6.12 Information security events and weaknesses

All information security events and suspected weaknesses are to be reported via the IT Helpdesk, for the attention of the Information Security Manager. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events.

6.13 Classification of Sensitive Information.

A consistent system for the classification of information within the NHS organisations enables common assurances in information partnerships, consistency in handling and retention practice when information is shared with non-NHS bodies. [NB. New guidance is being developed that is aimed to achieve consistency of information handling practice throughout the NHS].

Worcestershire NHS community shall implement appropriate information classifications controls, based upon the results of formal risk assessment and guidance contained within the IG Toolkit to secure their NHS information assets.

The classification **NHS Confidential** – shall be used for patients’ clinical records, patient identifiable clinical information passing between NHS staff and between NHS staff and staff of other appropriate agencies. In order to safeguard confidentiality, the term “NHS Confidential” shall **not** be used on correspondence to a patient in accordance with the Confidentiality: NHS Code of Practice. Documents so marked shall be held securely at all times in a locked room to which only authorised persons have access. They shall not be left unattended at any time in any place where unauthorised persons might gain access to them. They should be transported securely in sealed packaging or locked containers. Documents marked NHS Confidential not in a safe store or in transport should be kept out of sight of visitors or others not authorised to view them.

The classification **NHS Restricted** - shall be used to mark all other sensitive information such as financial and contractual records. It shall cover information that the disclosure of which is likely to:

- adversely affect the reputation of the organisation or it’s officers or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
• breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
• breach statutory restrictions on disclosure of information;
• disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.
NHS Restricted documents should also be stored in lockable cabinets

6.14 Protection from Malicious Software

The organisation shall use software countermeasures and management procedures to protect itself against the threat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organisation’s property without permission from WHICTS. Users breaching this requirement may be subject to disciplinary action.

6.15 User media

Removable media of all types that contain software or data from external sources, or that have been used on external equipment, require the approval of WHICTS before they may be used on Trust systems. Such media must also be fully virus checked before being used on the organisation’s equipment. Users breaching this requirement may be subject to disciplinary action.

6.16 Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis.

The Trust has in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees’ electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security
- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.
Any monitoring will be undertaken in accordance with the above act and the Human Rights Act
6.17 Accreditation of Information Systems

The organisation shall ensure that all new information systems, applications and networks include a security plan and are approved by the [insert appropriate security officer] before they commence operation.

(Organisations are encouraged to develop a series of System Level Security Policies (SLSPs) for systems under their control in order to distinguish between the security management considerations and requirements of each. In this way, specific responsibilities may be assigned and obligations communicated directly to those who use the system. A separate illustrative template will be provided to aid the local development of these SLSPs).

6.18 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by WHICTS.

6.19 Intellectual Property Rights

The organisation shall ensure that all information products are properly licensed and approved by WHICTS. Users shall not install software on the organisation’s property without permission from the WHICTS. Users breaching this requirement may be subject to disciplinary action.

6.20 Business Continuity and Disaster Recovery Plans

The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks.

6.21 Reporting

The Information Security Officer shall keep the Countywide and individual Trust and IG Steering Groups informed of the information security status of the organisation by means of regular reports and presentations.

6.22 Policy Audit

This policy shall be subject to audit by CW Audit.

6.23 Further Information

Further information and advice on this policy can be obtained from Ruth King, Information Security Manager, ruth.king@worcsacute.nhs.uk
7. Implementation

7.1 Plan for Dissemination

As detailed in key document, held in control document, WHICTS will ensure this policy is sent to each Trust’s Information Governance Manager who will arrange for it to be communicated through their appropriate channels - including all directorate managers within the Trust, whose responsibility it will then be to ensure that all staff groups within their area are directed to this policy. Information Security will also participate in the Information Governance workshops which will be held regularly.

7.2 Dissemination

This policy will be available on the Trust Intranet. A notice board link will be sent out to each Trust’s staff via email. The Head of Information/Information Governance will send the link for this policy to all Directorate managers and ask that it is disseminated to all staff groups.

7.3 Training and awareness

This Policy will be promoted by WHICTS including the training department and Information Security manager; each Trust’s Information Governance Team will also promote the Policy. This Policy will also be included, along with the Information Security Policy, as a requirement for any new staff member to sign up to via the User Declaration. Any key amendments to the Policy will be notified to each Trust for communication to staff groups.

8. Monitoring and Compliance

Any breaches in Policy will be identified and reported, initially logged as a call via the Service Desk and where appropriate an Incident being raised and investigated as per each Trust’s guidelines.

9. Policy Review

The Information Security Manager will ensure that any updates or new legislation will be reflected in this policy and disseminated throughout the Trust if changes are made prior to the next revision of the policy, due in 24 months from approval.
10. References

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Management: NHS Code of Practice - DH</td>
<td>Apr 07</td>
</tr>
<tr>
<td>Computer Misuse Act</td>
<td>1990</td>
</tr>
<tr>
<td>Criminal Justice and Public Order Act</td>
<td>1994</td>
</tr>
<tr>
<td>Copyright, Designs and Patents Act</td>
<td>1988</td>
</tr>
<tr>
<td>Data Protection Act/ Processing of Sensitive Personal Data Order</td>
<td>1998/2000</td>
</tr>
<tr>
<td>The Health and Safety at Work Act</td>
<td>1974</td>
</tr>
<tr>
<td>Human Rights Act</td>
<td>1998</td>
</tr>
<tr>
<td>Interception Of Communications Act</td>
<td>1985</td>
</tr>
<tr>
<td>Regulation of Investigatory Powers</td>
<td>2000</td>
</tr>
<tr>
<td>Trade Mark Act</td>
<td>1994</td>
</tr>
<tr>
<td>Common Law Duty of Confidentiality</td>
<td></td>
</tr>
<tr>
<td>Access Control Policy - WHICTS</td>
<td>Dec 10</td>
</tr>
<tr>
<td>Internet and Email Access Policy</td>
<td>Sept 09</td>
</tr>
<tr>
<td>Anti-Virus Policy</td>
<td></td>
</tr>
<tr>
<td>Home Working Policy</td>
<td></td>
</tr>
<tr>
<td>Mobile Computing Guidance</td>
<td></td>
</tr>
<tr>
<td>Network Security Policy</td>
<td></td>
</tr>
<tr>
<td>Safe Haven Policy</td>
<td></td>
</tr>
</tbody>
</table>

11. Background

11.1 Consultation

The following stakeholders have been consulted during the production of this Policy:
- WHICTS
- Information Governance Groups at Trust and County level
- Trust’s Counter Fraud Managers

11.2 Approval process

As a WHICTS Policy each Trust will co-ordinate approval via their IG Steering Groups and any additional identified committees, as detailed in the Checklist for the Review and Approval key document held in control document.

11.3 Equality Requirements

No potential discriminatory impact has been identified as a result of the Equality Impact Assessment Tool, so not required to refer to Human Resources, key document is held in control document.

11.4 Financial Risk Assessment

No business case has been completed as nothing highlighted as a result of the Financial Risk Assessment, key document held in control document.
12. Appendices

Appendix 1

1. Users Responsibility Statement

1.1 The purpose of this document is to summarise the key user responsibility requirements as laid out in the following documents:

- Information Security Policy
- Internet and E-Mail Access Policy
- Mobile Computing Policy
- Anti Virus Policy
- Relevant Trusts Incident Reporting Procedure
- Access control Policy
- Safe Haven Policy
- Equipment Disposal Policy
- Home working Policy
- Code of Conduct for Employees in Respect of Confidentiality

1.2 These documents support the organisation's overall Information Security Policy which sets out guidelines within the framework of the DH Information Security Management: NHS Code of Practice (April 2007). It is your manager’s responsibility to ensure that you are aware of those policies which are relevant to your role within the organisation.

1.3 The purpose of the Policy is to preserve:

- **Confidentiality** – Access to data is confined to those who have legitimate authority to view it.
- **Integrity** – Data is timely and accurate and detected or amended only by those specifically authorised to do so.
- **Availability** – Data is available to those authorised when it is needed

By following the guidelines in this statement the users can minimise risks in relation to information security. Non-compliance may result in disciplinary action being taken in accordance with relevant Trust's disciplinary policy, and may lead in very serious cases to dismissal for gross misconduct, as detailed in your Trusts Code of Conduct for Employees in Respect of Confidentiality.

To obtain a copy of the disciplinary policy please discuss with your manager or the Human Resources department.
2. Safeguarding Data - IT Security Essentials

- Use your own password, ensure that it is kept secret at all times and never use somebody else’s.
- Don’t leave computers open for unauthorised access, ensure either logged out or locked (Ctrl+Alt+Delete) when unattended.
- Only share person identifiable data with those who are authorised to see it.
- Save all data to network drives, e.g. M drive, not to your C:\ drive as network data is secure and backed up.
- Do not hold Person Identifiable Data (PID) on portable media (including laptops) unless it is encrypted. Please contact the IT department for further guidance.
- Ensure that laptops are backed up regularly to a network drive and that they are logged onto the network regularly to receive antivirus and other major updates.
- Only send patient identifiable information, outside WHICTS, through NHSmail i.e. between email addresses that end in nhs.net. Alternatively the data must be encrypted.
- Do not use the internet inappropriately.
- Do not load unofficial software onto Trust computers (including laptops)
- All mobile devices should be password protected and laptops should be encrypted, with WHICTS software.
3. **Caldicott Principles**

The Caldicott Report set out a number of general principles that health organisations should use when reviewing its use of client information and these are set out below:

**Principle 1: Justify the purpose(s)**

Every proposed use or transfer of personally identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appropriate guardian.

**Principle 2: Do not use personally identifiable information unless it is absolutely necessary.**

Personally identifiable information items should not be used unless there is no alternative.

**Principle 3: Use the minimum personally identifiable information.**

Where the use of personally identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiably.

**Principle 4: Access to personally identifiable information should be on a strict need to know basis.**

Only those individuals who need access to personally identifiable information should have access to it.

**Principle 5: Everyone should be aware of their responsibilities.**

Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and obligations to respect patient/client confidentiality.

**Principle 6: Understand and comply with the law.**

Every use of personally identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.
User Responsibility Declaration

I confirm that I have read and understood the content of the Information Security Policy, the Internet and Email Access Policy and any other Policies relevant to my role. By doing this I therefore accept responsibility for maintaining security and confidentiality within my working practices.

I acknowledge that wilful disregard for this policy in my actions may make me liable for action in accordance with the Organisation’s disciplinary procedures.

On completion below, I confirm that I will adhere to the content of this statement.

<table>
<thead>
<tr>
<th>Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Department</td>
<td></td>
</tr>
<tr>
<td>Trust</td>
<td></td>
</tr>
<tr>
<td>Date of Acceptance</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
<tr>
<td>Name of line manager</td>
<td></td>
</tr>
</tbody>
</table>

Your line manager should retain a signed copy, to be held in your personal file, and an electronic copy should be mailed from your mailbox to:

WHICTS.InformationSecurity@worcsacute.nhs.uk