NHS
North Yorkshire and York

Title:	**SAFE HAVEN POLICY**
Reference No:	**NHSNYYIG - 006**
Owner:	Director of Standards
Author:	Information Governance Team
First Issued On:	March 2009
Latest Issue Date:	February 2012
Operational Date:	February 2012
Review Date:	April 2013
Consultation Process:	Via Information Governance Steering Group
Policy Sponsor:	Information Governance Steering Group
Ratified and Approved by:	Governance and Quality Committee
Distribution:	All Staff
Compliance:	Mandatory for all permanent and temporary employees, contractors and sub-contractors of NHS North Yorkshire and York
Equality & Diversity Statement	

CHANGE RECORD			
DATE	AUTHOR	NATURE OF CHANGE	VERSION No
Dec 2008	Information Governance Officer	New policy draft.	0.001
Jan 09	Info Gov Team	Forwarded to AD IM&T and Records Management Consultant for initial comment.	0.001
Jan 09	Info Gov Team	Updates re audit of Safe Haven procedures.	0.002
Feb 09	Info Gov Team	Final Version	1.00
Dec 11	Info Gov Team	Updated to reflect new organisational structure	1.01

© NHS North Yorkshire and York 2009

CONTENTS

PREFACE

This Policy is made between North Yorkshire and York Primary Care Trust (NYY PCT; “the PCT”) and the recognised staff side organisations, using the mechanism of the Joint Negotiation and Consultative Committee (JNCC). It will remain in force until superseded by a replacement Policy, or until terminated by either management or staff side, giving no less than six months notice. The purpose of the notice to terminate the Policy is to provide the opportunity for both parties to renegotiate a replacement Policy. Withdrawal by one party, giving no less than six months notice, will not of itself invalidate the agreement. If agreement cannot be reached on a revised policy, then either party may refer the matter to the Advisory, Conciliation and Arbitration Service (ACAS) for conciliation.

Document Objectives

This policy is a consolidation of the existing Safe Haven Policies from the four PCTs which were merged into the North Yorkshire and York PCT in 2006, and sets out the approach taken within the Trust to provide a robust Safe Haven procedure for the current and future management of information.

Intended Recipients

All staff with record management responsibilities.

1. INTRODUCTION

The NHS constantly uses and transfers information between people, departments and organisations much of this information is sensitive and/or personal and requires treating with appropriate regard to its security and confidentiality. It is therefore essential that all departments and services within the PCT put in place adequate safe haven procedures to protect information:

- At the point of receipt,
- whilst held by the department,
- when transferring information to others, by what ever means,
- when archived, and
- at the point of disposal.

This document sets out the framework within which the staff responsible for handling person identifiable or corporate confidential information can develop procedures to ensure that this information is handled, transferred, stored and disposed of securely.

2. SCOPE

This policy relates to all flows of confidential information, clinical and non-clinical unless otherwise stated, that are created, received, maintained, stored, transferred or destroyed by staff working for or on behalf of NHS North Yorkshire and York (NHS NYY)

It must be followed by all staff who work for the Trust, including those on temporary or honorary contracts, pool staff and students. Access and the level of access, to confidential information should be granted on a strict 'need to know' principle as specified by the Caldicott Principles. This should be no more than necessary for the recipient to carry out the legitimate activities for their job.

Breaches of this procedure may lead to disciplinary action being taken against the individual concerned.

Independent contractors are responsible for the management of their information flows and for ensuring compliance with relevant legislation and best practice guidelines. The Trust is happy to provide such advice and support as required.

3. DEFINITIONS

a. **Safe Haven –** in security terms a Safe Haven is a work location e.g. an office or work area, entry to which is restricted to authorised persons, suitable for the receipt and transmission of sensitive information keeping that information protected at all times. A Safe Haven must have a nominated manager, adequate security to prevent unauthorised access and be staffed by employees how are trained and confident in sending and receiving sensitive information.

b. **Personal Information** – this is information about an individual which would enable that individual's identity to be established. This might be fairly explicit such as a name or address or items of different information which if taken together or put together with information already in the public domain could allow an individual to be identified. All information that relates to an attribute of

an individual should be considered as potentially capable of identifying them to a greater or lesser extent. Examples are:

- **Name or Initials**
- **Address**
- **Postcode**
- **Date of Birth**

GP

- **GP**
- **Gender**
- **NHS or hospital number**

c. **What is Sensitive Information? -** this can be broadly defined as information about an individual whose release could case harm or distress to individuals, organisations or the wider community. Examples of such information would include:

- **Health records**
- **Financial information**
- **Religious beliefs**
- **Racial / ethnic origin**
- **Political opinions**
- **Membership to unions**
- **Sexual life**
- **DNA or fingerprints**
- **Social Services material**

d. **Information Processing:-** means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data;

e. **Caldicott Principles -**The Caldicott report relates to the use of patient-identifiable information within the NHS and highlighted two key points:

- All NHS organisations must appoint a Caldicott Guardian, and
- Details six key principles to be applied when using patient –identifiable information.

Compliance with these principles reduces the risk of breach of confidentiality and breaching the Data Protection and Human Rights Acts. These principles detail best practice and should therefore also be adopted when dealing with all personal information and confidential corporate information.

The 6 Caldicott Principles

1. Justify the purpose for using patient-identifiable information
2. Only use information when absolutely necessary
3. Use the minimum that is required for the purpose.
4. Access should be on a need to know basis
5. Everyone must understand their responsibilities
6. Understand and comply with the law.

f. **Information flows: –** these are routine transfers of information either to other departments within the PCT or to other organisations and contain sensitive or person identifiable information.
The information flow mapping tool is available at:
http://nww.nyypct.nhs.uk/Corporate/InformationGovernance/DataAuditTool.htm

4. Roles and Responsibilities

Chief Executive

The Chief Executive has overall responsibility for the implementation of Safe Haven Procedures within the Trust. As Accountable Officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Safe Haven implementation is key to this as it will ensure that personal and confidential information is handled securely.

The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

Caldicott Guardian

The Caldicott Guardian is responsible for the review and agreement of internal procedures governing the protection and use of patient-identifiable information by staff. In addition they are responsible for the review and agreement of protocols governing the disclosure of information across organisational boundaries in conjunction with the Information Governance Steering Group.

Information Governance Steering Group

This group is responsible for the review and agreement of internal procedures governing the protection and use of all other personal information, e.g. staff, and Trust confidential information.

Service Managers / Line Managers

- Identify all areas that need to be classified as safe havens within their departments.
- Nominate a member of staff to manage the safe haven area.
- Ensure all staff are aware of this policy and that department/service safe haven procedures are developed and implemented.

Nominated Safe Haven Managers

- Ensure access is properly restricted to required staff only
- Identify routine information flows and ensure that these are mapped.
- Develop safe haven procedures specific to the area / service
- Ensure all staff are fully aware and trained in confidentiality and safe haven procedures.
- Display guidance posters as necessary.
- Regularly review the adequacy of controls in place and amend where necessary.

Staff

- Ensure they are aware of, understand and adhere to procedures,
- Ensure that any transfer of information is in accordance with Data Protection Act, NHS Code of Confidentiality and Caldicott Principles.
- Wear ID badges if issued
- Query the status of strangers
- Report any suspicious or worrying situations.
- Highlight areas of potential weakness to their nominated safe haven managers.

5. Safe Haven Procedures.

It is the Trusts policy that all areas handling confidential personal identifiable information, both of patients and others, and confidential corporate information must be secure and have adequate controls in place to protect information at all times. In order to ensure confidential information remains adequately secure all areas using such information must be identified and have documented and implemented adequate safe haven controls.

5.1. **Identifying where safe haven procedures should be implemented.**

Any area that creates, collects, holds, or transfers personal identifiable information or confidential corporate information must be designated a Safe Haven area. All Safe Haven areas must have a nominated safe haven manager and document and implement safe haven procedures.

5.2. **Nominating a Safe Haven Manager**

It is essential that an appropriate manager is nominated and delegated with the responsibility for ensuring that safe haven procedures are documented and implemented, and that staff are trained properly trained in safe haven procedures. This manager must have a full understanding of information confidentiality and security requirements.

5.3. **Establishing security and controls**

The Nominated Safe Haven Manager must review the information processed by their service and ensure that adequate controls are in place to protect this information. Regular information flows must be documented on the information flow mapping tool at: http://nww.nyypct.nhs.uk/Corporate/InformationGovernance/DataAuditTool.htm.
Managers must also identify the types of ad-hoc flows of information and the sensitivity of other information held by the department.
The existing controls to protect personal and confidential information must be reviewed for adequacy, gaps identified and a corrective action plan formulated. Where possible corrective action must be implemented immediately, if corrective action can not easily be taken the weaknesses must be reported on the risk register and an action plan with completion dates filed.

5.4. **Documenting safe haven procedures**

Safe Haven procedures implemented must be documented and be available to staff for reference purposes. A copy of these procedures must be returned to the information governance team and may be subject to audit.

5.5. **Training Staff**

All Trust staff will be made aware of their responsibilities in respect of the departmental safe haven procedures and transferring of information.

5.6. **Security Breaches**

Any breaches in security or losses of information must be reported via the incident reporting system.

5.7. **Reviewing and updating safe haven procedures.**

Safe Haven procedures must be reviewed and updated on an annual basis or a record or no change required made.

6. Safe Haven Procedures Audit

The Trust will regularly audit safe haven procedures for compliance with this framework.

6.1 Audits will:

- Identify areas of operation that are covered by the Trust's policies and identify which procedures and/or guidance should comply to the policy;
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the use, transfer and storage of information, and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance; and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures

6.2 There are two types of records audit that must be carried out on a regular basis:

6.2.1 Safe Haven Procedures Audit

It is the Trusts policy that Safe Haven procedures will be audited regularly, either specifically or as part of a general Information Governance Audit to ensure that all services have adequate controls in place to protect person identifiable and other confidential information. This audit is led by the Information Governance Team

6.2.2 Information Flows Audit

As part of the Information Governance Assurance Programme, all NHS organisations and are required to have an up-to–date register of the information they hold and understand how it is handled and transferred to others. To compile this register the PCT needs to audit across the whole PCT. This audit is led by the Information Governance Team.

7. Review and Retention

This policy will be reviewed one year after its initial issue and every two years thereafter. (or sooner if new legislation, codes of practice or national standards are to be introduced)

This policy will be retained in line with the Records Management: NHS Code of Practice (Dept of Health 2009) retention schedules.

8. Equality and Diversity Statement

The PCT recognises the diversity of the local community and those in its employ. Our aim is therefore to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need. The PCT recognises that equality impacts on all aspects of its day to day operations and has produced an Equality and Human Rights Strategy and Equal Opportunities Policy to reflect this. All strategies, policies and procedures are assessed in accordance with the Equality & Diversity Assessment Toolkit, the results for which are monitored centrally.

9. Disciplinary Statement

Breaches of this policy will be investigated and may result in the matter being treated as a disciplinary offence under the Trust's disciplinary procedure.

10. References

Department of Health (2006*). Records Management: NHS Code of Practice: Parts 1 & 2*. [Online] [27.08.08]. Available from World Wide Web www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/Browsable/DH_4133200

Department of Health (2003). *Confidentiality: NHS Code of Practice*. [Online] [27.08.08]. Available from World Wide Web www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

The Common Law Duty of Confidentiality [Online] [27.08.08]. Reference to available from World Wide Web www.dh.gov.uk/en/Policyandguidance/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4084181

The Data Protection Act (1998). [Online] [27.08.08]. Available from World Wide Web www.opsi.gov.uk/acts/acts1998/19980029.htm

Information minimum security measures. Available on the Trusts intranet at: http://nww.nyypct.nhs.uk/Corporate/InformationGovernance/docs/GuidelinesPolicies/5-8%20-%20NYY%20PCT%20-%20Minimum%20Security%20Meaures%20Table%20Vers%201.22%20-%2020081008.pdf

Information Flow Mapping Tool. Available on the Trusts intranet at: http://nww.nyypct.nhs.uk/Corporate/InformationGovernance/DataAuditTool.htm

ANNEX A

Quick guide on how to develop Safe Haven Procedures

1. Identify areas that hold and use personal identifiable and corporate confidential information.
2. Nominate a manager of appropriate seniority and knowledge as the safe haven manager
3. Identify both routine flows and ad-hoc information flows
4. This manager must then develop comprehensive safe haven procedures for the service or department as follows:
    a. Complete Information Mapping Tool for all regular information flows and return a copy to InfoGovmatters@nyypct.nhs.uk.
    b. Complete the proforma ANNEX B
    c. Identify controls already in place and areas of weakness. Implement corrective action that can be undertaken immediately.
    d. Document controls already in place and new ones implemented as safe haven procedures.
    e. Make all staff aware of these procedures and their respective responsibilities
    f. Develop a corrective action plan for weaknesses that can not be immediately solved.
    g. Report weaknesses in information security via the risk register and devise and report a corrective action plan, including completion dates.

5. Ensure a copy of the procedures are available to staff at all times for reference and return a copy to Information Governance Team
6. Under take an annual review of procedures in place to ensure that procedures remain appropriate. Where changes are made return a copy to the Information Governance Team, where no changes are made record date of review and that the procedures have not been subject to change.

ANNEX B

Developing Safe Haven Procedures Questionnaire

Security of the Safe Haven Area					
No.	**Question**	**YES/NO**	**Corrective action**	**Action Date**	**Notes**
1	Is the area separated from the general public by two access controls when unmanned, e.g. two locked doors or a locked door and all personal information is locked away.				
	Is the area protected by an alarm system out of hours?				If No advice should by sought from the Trusts Security Manager
	Is access to this area restricted to those who work in that area?				
	If the area is a shared area are staff aware that minimum information should be out at any time and put away as soon as it is finished with. It must also not be left in view of unauthorised staff				Any shared areas must be reported as a weakness and review made to try and locate a secure location.
	In the event that unauthorised personnel require access to the safe haven area are they accompanied at all times and all personal information removed from view?				
	Are staff aware that the area must be locked if it is to be left unattended?				
	Where keypad locks are in place are the codes changed on a regular basis, i.e. quarterly?				
	Are all staff aware and fully trained of information handling, transferring, sharing and security requirements?				See training presentations on the Information Governance Intranet Page
Security of Manual Records					

	Is information in what ever format restricted to those who need to know it to do their job?				**NB.** Being an NHS employee does not in itself qualify an individual as needing to know.
	Has a clear desk policy been implemented?				This must be a control built into the safe haven procedures for the area
	Are all files containing personal information held securely when not in use? E.g. in locked filing cabinets or drawers				See Records Management Policy Information and Minimum Security Measures and document the appropriate measures for you area
	Is access to files containing personal information etc. restricted to staff who need them to legitimately do their job?				See Records Management Policy
	Are Records filed in such a manner that they can be quickly located if required?				See Records Management Policy
	Has a tracking / tracing system been implemented?				See Records Management Policy
	Are records held securely within files? E.g. bound				See Records Management Policy
	Is it ensured that all confidential information is not visible through or on the files cover?				See Records Management Policy
	When copies of records are transferred is a record of that transfer maintained, to whom, and why?				See Records Management Policy
Security of Computer Records					
	Are monitors placed so that information displayed on them can not be overseen? E.g. through a window or in an open reception area				
	Have processes been put in place to ensure that information is saved to a main server and not the local computer?				
	Have all system users been issued with individual passwords to the systems they				

	require, limiting them only the information they require to do their job				
	Are staff aware of there responsibilities in respect of passwords and systems access				See acceptable use policy
	Are all staff aware that they must lock their computer or log out when leaving it unattended?				
Encryption.					
	Where electronic storage media are used e.g. laptops, PDAs, messages on phones etc. has it been ensured that adequate encryption has been installed and is in use.				See Information Minimum Security Measures and document the appropriate measures for you area. For assistance contact ITServiceDesk@nyypct.nhs.uk.
Protective Markings					
	Has the service/department implemented the use of protective markings?				See Information Minimum Security Measures and document the appropriate measures for you area
White Boards					
	Where white boards are in use have they been placed in areas that can be over seen by the public or unauthorised personnel?				
	Is it policy to ensure that information recorded on white boards is anonymised?				
	Is it policy to record only the minimum information required on white boards?				
Transferring Information					
	Are Staff aware of both the NHS Code of Confidentiality and Caldicott principles?				
	Have appropriate staff been authorised to transfer information?				See Information Minimum Security Measures and document the appropriate measures for you area
	Are staff aware of situations where the data subjects consent is required before information can be transferred?				

	Have secure methods of transfer appropriate to the information being transferred been determined and implemented?				
Staff taking information off Trust premises.					
	Do staff needing to remove confidential information from Trust premises obtain the appropriate approval to do so and is this approval recorded?				See Information Minimum Security Measures and document the appropriate measures for you area
	Is a record made of information taken off site?				
	Is it ensured that only the minimum required is transported?				
	Are staff aware that they are bound be the same rules of confidentiality and must keep records safe and secure at all times whilst away from their place of work?				
	Has a tracer system been implemented to record the removal of files?				
	Have appropriate transportation methods been implemented? E.g. carried in a locked container case to ensure nothing is lost.				
	Are staff aware that when records are to be transported and on occasions left in vehicles that they must be out of sight and in a locked container and must comply with the Records Management Policy. **NB/** Records must never be left in vehicles for long periods, e.g. over night				Should this be necessary it must be recorded and bought to the managers attention beforehand and must be locked in the car boot, in a locked container
	Are staff aware that records are not to be left in easily accessible areas in whatever format?				
	Are staff aware that when records are taken home care must be taken to ensure they are safe and not accessible to other members of				

	the household or visitors?				
	Is it ensured that records are returned to Trust premises as soon as possible?				
Identifying Information Flows					
	Does your department send routine reports or bulk amounts of information to other departments or organisations?				
	Have these information flows been mapped?				See Information Flow Mapping Tool.
	Have appropriate controls been implemented to protect this information in transit?				
Mail – Incoming					
	Are staff aware letters marked safe haven must not be opened by other than an authorised member of staff?				
	Is correspondence containing personal or sensitive material locked away when the safe haven in unattended?				
	Are staff aware any safe haven correspondence received in error must be resealed and forwarded immediately to the correct recipient or if not know returned to sender. Ensuring the packaging is marked **Safe Haven, Private and Confidential**				
Mail – Outgoing					
	Are staff aware that all outgoing letters are marked **private and confidential –safe haven addressee only?**				See Information Minimum Security Measures and document the appropriate measures for you area
	Are Staff aware of the correct packaging methodologies for confidential information being sent out?				
	Are Staff aware of the correct method for sending confidential information being sent out, e.g. courier, post or by hand?				
	Is all outgoing mail marked **Private and**				

	Confidential to be opened by addressee only.				
Couriers					
	Does your service use couriers where it has been determined that the postal system is not sufficiently secure?				See Information Minimum Security Measures and document the appropriate measures for you area
Fax					
	Is the fax machine situated in a secure area and access to it is only available to authorised staff.				See Information Minimum Security Measures and document the appropriate measures for you area
	The fax is a dedicated safe haven only fax and used only for safe haven purposes.				
Incoming Faxes					
	Are incoming faxes collected regularly by authorised staff?				See Information Minimum Security Measures and document the appropriate measures for you area
	Is it standard practice to store incoming faxes in the fax machine buffer out of hours ready for printing by an authorised member of staff?				
	Are staff aware that faxes containing personal information incorrectly received must be placed in a sealed envelope, marked appropriately as per mail above and forwarded to the addressee of the fax?				
Outgoing Faxes					
	Are key Safe Haven faxes numbers pre-programmed into the machine to avoid misdialling?				See Information Minimum Security Measures and document the appropriate measures for you area
	Do staff know to double check individually keyed numbers before sending?				
	Do staff make the recipient aware of the transmission of a fax when sending to a none pre-programmed number requesting acknowledgement of receipt?				
	Are faxes marked **PRIVATE AND**				

	CONFIDENTIAL and is the address checked prior to sending?				
	Are staff aware to use the minimum patient details possible e.g. using NHS Number in place of the patients name?				
Email – Incoming.					
	Do staff remove emails containing personal information from their email system and file securely as soon as possible?				**NB**, personal information should not be held on email system longer than absolutely necessary.
	If there is a more formal method of communication e.g. a web based referral system, are staff aware that this must be used in place of email.				
Email – Outgoing					
	Do staff consider whether email is the most appropriate method to send the information – can another method be used? **Nb/** Emails can easily be forwarded to others against your wishes.				See Information Minimum Security Measures and document the appropriate measures for you area
	Are recipients of the email kept to a minimum and are these recipients checked to ensure they are the correct ones before the Email is sent.				This can be done be checking the properties of the recipients address?
	Are Staff aware the any emails containing personal information must be sent from and to an NHS Mail account? The documents must be password protected. The password to be communicated separately from the email – i.e. by phone.				See Information Minimum Security Measures and document the appropriate measures for you area
	Do staff ensure that the minimum information is sent for the recipient to be able to carry out their job?				
	Are staff aware that they must never use				

	personal identifiable information in the subject line?				
	Do staff mark the Emails **CONFIDENTIAL?**				
	Is a disclaimer placed on the email stating that the recipient is responsible for the security and confidentiality of the data within that email and that data must not be passed on to others via any method unless they have a justified need to know?				
Telephones Conversations					
	Are all staff aware that any conversations regarding personal or confidential information must take place in a safe haven area or other place where they can not be over heard?				
	When speaking to service users or careers do staff confirm the caller's identity or call back?				
	Are staff aware to use the secrecy button when putting callers on hold?				
	When telephone messages are taken are they put in an envelope, sealed and addressed to the recipient marked private and confidential?				
	In the event of requests for information by telephone do staff confirm the identity of the requestor and their authorisation to receive the information? This could mean calling the enquirer back via a main switch board **DO NOT** use direct lines for this verification purpose				
Answer Phones – Incoming					
	When checking messages on an answer phone ensure they can not be overheard by unauthorised personnel?				
	If message books are used is it ensured that				

	these are held securely?				
Answer Phones – Outgoing					
	Are staff aware that in the event that they have to leave an answer phone message that they only request the contactee to call back leaving a name and phone number?				
Verbally transfer of information					
	Are staff aware that whenever they are transferring information verbally, either formally or informally that they must ensure they are not overheard. Where possible do not identify the service user?				
	Where service users registering at reception is it ensured that any personal details they need to give can not be overheard?				
	Where discussions must take place in a community area e.g. shared office or ward are staff aware that they are expected to respect patient's rights?				
	Where message books are used is it ensured that these are held securely?				
Information Sharing					
	Are staff aware of their responsibilities in respect of information sharing?				
	Are staff aware of guidance available i.e. the NHS Code of Confidentiality?				The NHS Code of Confidentiality is available on the Information Governance Intranet Page IG Policies and Guidelines
	Has responsibility for making Information sharing decisions been delegated?				
	Where information is shared with other agencies has an Information Sharing Protocol been put in place?				
Subject Access Requests					

	Have staff been made aware for their responsibilities in respect of patients requesting copies of medical records?				Department of Health Guidelines available on the Information Governance Intranet Page IG Policies and Guidelines
	Are staff able to advise service users on how to apply for a copy of their records?				
	Are all records reviewed by an appropriate clinician to ensure no exempt information is sent out? E.g. third party information				
Out of Hours					
	Have Out of Hours situations been reviewed to ensure that adequate security has been implemented for all of the above.				
Disposal of Information					
	Have the correct methods of disposing of information securely and confidentiality whatever its format have been identified and implemented?				
Reporting Incidents					
	Are staff aware that all breaches of information or safe haven area security or confidentiality must be reported, including near misses?				See Information Minimum Security Measures and document the appropriate measures for you area
Highlighting Security weaknesses					
	Are staff aware that they are responsible for reporting security weaknesses to their manager for corrective action?				
Documented Procedures					
	Have the controls identified in completing this questionnaire been documented and communicated to staff?				See Policy on policies for format
Training					
	Have staff been trained in these procedures?				See Information Minimum Security Measures and document the appropriate measures for you area