Policy Title and ID number	**SAFE HAVEN POLICY** **ID Code: (GEN IT 6.13)**			
Sponsoring Director:	**Director of Quality and Standards**			
Implementation Lead:	Information Governance Manager			
Impact:	*(a) To patients*	None		
	(b) To Staff	Yes		
	(c) Financial	None		
	(d) Equality Impact Assessment (EIA)	Completed: **Yes**		
	(e) Other	None		
Additional Costs:			*Budget Code*	*Revenue or Non Revenue*
	(a) Training:	*£0*		
	(b) Implementation:	*£0*		
	(c) Capital:	*£0*		
	(d) Other	*£0*		
Training implications:	*To be incorporated into induction:* **Yes**		*Other:*	
Date of consultation at:	*Board of Directors*		For Note: January 2011	
	Executive Team			
	Divisional Medical Directors/Clinical Directors			
	Assistant Divisional Directors/Heads of Department			
	Non Clinical Governance & Risk Committee		*7th December 2010*	
	Joint Partnership Forum		*14th December 2010*	
	Local Negotiating Committee		*N/A*	
	Infection Control Committee:		*N/A*	
	Health & Safety Committee		*N/A*	
	Barnsley Information Group		*28th October 2010*	
Alignment	*HR:*		Yes	
	Strategic Direction:			
	Board Assurance:		Yes	
	Clinical Governance:			
Date of Final Draft:	*December 2010*		Issue Number:	2.0
Date of Final Approval:			Approved by:	by Trust Board
Implementation Date:	*February 2011*			
Date of last review:	*February 2011*	Date of next review:	February 2013	
Circulation Date:				
Circulation:			Yes	Comment
	Directors		Yes	
	Non Executive Directors		Yes	
	Divisional Medical Directors/Clinical Directors		Yes	
	Medical Staff Committee/SMSF		Yes	
	Assistant Divisional Directors		Yes	
	Assistant Nursing Directors		Yes	
	Heads of Department		Yes	
	H&S Committee Members		Yes	
	Policy database/warehouse		Yes	
	Others (to be listed):		All Trust Staff	

SAFE HAVEN POLICY

DOCUMENT ID: GEN IT 6.13

October 2010

SPONSORING DIRECTOR: DIRECTOR OF Quality and Standards

SAFE HAVEN POLICY

CONTENTS

Summary

1. Policy Aim
2. Introduction
3. Policy Scope
4. Code of practice for Sending Confidential Information
5. Code of Practice for receiving confidential Information
6. Responsibilities
7. Related policies

Document ID: GEN IT 6.13

SAFE HAVEN POLICY

1. Introduction

A Safe Haven is a term used to describe arrangements that are in place in an organisation to ensure that confidential information is communicated safely and securely.

In order to comply with legislation and DOH guidance, all NHS organisations are required to operate Safe Haven procedures to safeguard the confidentiality of personal data or other sensitive information.

This policy specifies the procedures to be followed by BHNFT staff when transmitting or receiving confidential or sensitive information by post or fax.

This policy applies to the receipt or transfer of information where a duty of confidence applies and also to other non-personal information considered sensitive by the organisation.

A duty of confidence will apply to:

- All patient/client information
- Staff information held by Human Resources & Occupational Health

2. Policy Aim

In order to comply with legislation and DoH guidance, all NHS organisations are required to operate Safe Haven procedures to safeguard the confidentiality of personal data or other sensitive information.

The aim of the policy is to ensure that Barnsley Hospital NHS Foundation Trust (BHNFT) operates such procedures, ensuring that confidential or sensitive information sent to or from BHNFT is handled in such a way as to minimise the risk of inappropriate access or disclosure.

This policy ensures compliance with:

- The Data Protection Act 1998
- Common Law of Confidentiality
- Confidentiality: NHS Code of Practice
- Caldicott Recommendations

3. Policy Scope

A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. Confidential information must not be disclosed in a way that the person providing that information is not aware of, unless the law requires otherwise.

A duty of confidence **will apply** to:

- All patient/client information
- Staff information held by Human Resources & Occupational Health

This policy applies to the receipt or transfer of all information where a duty of confidence applies and also to other non-personal information considered sensitive by the organisation.

4. Code of Practice for Sending Confidential Information

4.1. Always consider whether it is necessary to release Person Identifiable Data (PID) for care purposes

4.2. All transfers of patient/staff data for non-care purposes must be anonymised by using either NHS Number, Unit number or Employee number only.

4.3. Send PID only when it is essential to do so

4.4. Ensure that documents are properly 'booked out' of any relevant filing system if necessary, and records kept of what is sent and where. Copies should be sent or retained, as appropriate.

4.5. When sending paper documents outside of the NHS, send only to known, named authorised personnel marked 'Confidential'.

4.6. Unencrypted PID can only be sent securely between NHS mail accounts electronically. Valid NHS mail addresses always end in 'nhs.net'.

4.7. Documents with the appropriate level encryption (256 bit) can be sent outside of the nhs.net network (e.g. Local Government). (Please refer to NHS Mail acceptable use policy for up to date list of secure email addresses).

4.8. When sending documents by post or courier, use a 'signed for' delivery service. Use appropriate stationary, such as reinforced envelopes or document wallets when necessary. Check the address and ensure that it is transcribed in clear indelible ink.

NB: *In the exception where clinical risk and/ or patient safety requires the urgent transfer of PID and encryption tools are not available, this requires approval from either Caldicott Guardian, Senior Information Risk Officer, IG Manager or Duty Manager who will document and notify the Information Governance Department.*

5. Code of Practice for Receiving Confidential Information

5.1. All staff should arrange to receive confidential information through the Safe Haven Procedures.

5.2. Items arriving by post, hand or courier must be clearly marked 'Confidential'. They must either be handed personally to the recipient, an authorised alternative (such as a deputy or secretary) or held in a secure location until an appropriate member of staff is available.

5.3. Staff receiving confidential information in error should pass it to the correct recipient as soon as possible, observing the security measures above.

5.4. Where it is apparent that received mail or faxes, although not marked 'Safe Haven', do contain confidential information, the following procedure should be followed:

5.5. Documents must be placed in a sealed envelope marked 'Confidential', should be personally addressed and promptly delivered.

5.6. Transit envelopes and 'second' hand stationary should not be used

5.7. Receipt of confidential information in an inappropriate manner should be reported via the BHNFT's Risk and Incident reporting procedures.

5.8. Staff who regularly receive confidential material by fax should arrange for a Safe Haven fax number to be assigned to themselves/workgroup.

6. Responsibilities

All BHNFT staff must be aware of and follow the guidelines contained in this policy.

7. Related Policies

Confidentiality Policy
Data Protection Policy
Incident Reporting Policy & Procedures
Serious Untoward Incident Policy (SUI)

Appendix A

Caldicott Principles

The Caldicott Standards are based on the Data Protection Act 1998 principles and again are set out in the form of Principles

The Caldicott Guardian for the Trust is the Medical Director.

Principle 1: **Justify the Purpose**
Every proposed use or transfer of patient-identifiable
Information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate Guardian.

Principle 2: **Don't use Patient-Identifiable Information unless it is absolutely necessary**
Patient-identifiable information items should not be used unless there is no alternative

Principle 3: **Use the minimum necessary Patient-Identifiable Information**
Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability

Principle 4: **Access to Patient-Identifiable Information should be on a strict need-to-know basis**
Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see

Principle 5: **Everyone should be aware of their responsibilities**
Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are aware of their responsibilities and obligations to respect patient confidentiality

Principle 6: **Understand and Comply with the Law**
Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements