



FRAUD POLICY

Title:	Fraud Policy		
Author(s):	Mr Paul Nicholson, Assistant Director of Finance		
Ownership:	Finance and IT Directorate		
Date of SEMT Approval:	April 2016	Date of Trust Board Approval:	May 2016
Operational Date:	May 2016	Review Date:	May 2019
Version No:	TW/2/Fin (v5) 2016	Supercedes:	All previous versions
Key Words:	Fraud Policy		
Other Relevant Policies/Documents:	Fraud Response Plan Whistleblowing Policy Standing Orders, Standing Financial Instructions and Scheme of Delegation. NIAS HSC Trust Management Statement. Code of Conduct for HPSS Managers Standards of Business Conduct for HPSS Staff Bribery Policy		
Version:	TW/2/Fin (05) 2016		
(01) 1995-2008 (reviewed and updated regularly – previously entitled “Fraud Strategy and Fraud Response Plan	Evidence Base: Relevant legislation and literature used – Theft Act (Northern Ireland) 1969 The Theft (Northern Ireland) Order 1978		
(02) September 2008	Relevant legislation and literature used - The Fraud Act 2006 (introduced on 15 January 2007). This document should be read in conjunction with the Trust’s Fraud Response Plan. Published September 2008		
(03) November 2009	Reviewed and updated to reflect HSS(F) 07/2009, in particular the inclusion of Public Concern at Work details as a route to report concerns or get advice. Published April 2010.		
(04) December 2011	Contact numbers updated		
(05) March 2016	Reviewed annually and no material updates required. Updated formally for review by Audit Committee in May 2016 and consideration by Trust Board in June 2016. Main changes to contact numbers and transfer of responsibilities from DHSSPS to BSO CFPS.		

	(This policy is based on the Financial Governance Model Documents issues under HSS(F) 13/2007 and as such does not completely follow the format prescribed in the Trust's Policy on Development, Approval and Review of Trust Policies Version 1.0 approved in September 2014).
--	---

Circulation List:

This Policy was circulated to the following groups for consultation.

- Trade Unions
- Executive Directors and Senior Managers

Following approval, this policy document was circulated to the following staff and groups of staff.

- All Trust Staff

Trust Internet Site/Intranet Site

1.0 INTRODUCTION

- 1.1 One of the fundamental objectives of the Trust is to ensure the proper use of the public funds with which it has been entrusted. In pursuit of this objective, the Trust promotes an anti-fraud culture which requires all staff to act with honesty and integrity at all times and to take appropriate steps to safeguard resources.
- 1.2 The majority of people who work in the Trust and throughout the HSC are honest and professional and they rightly consider fraud to be wholly unacceptable. Nevertheless, fraud is an ever-present threat and must be a concern for members of staff and all stakeholders. Fraud may occur internally or externally and may be perpetrated by staff, external consultants, suppliers, contractors or development partners, individually or in collusion with others.
- 1.3 The purpose of this document is to set out the Trust's position on fraud and thereby set the context for the ongoing efforts to reduce fraud to the lowest possible level.

2.0 DEFINITION

- 2.1 The Fraud Act 2006 was introduced on 15 January 2007. Under the Act fraud is now a specific offence in law. The Fraud Act 2006 supplements the Theft Act (Northern Ireland) 1969 and the Theft (Northern Ireland) Order 1978. Fraud is used to describe acts such as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion.
- 2.2 For practical purposes, fraud may be considered to be the use of deception with the intention of obtaining an advantage, avoiding an obligation or causing

loss to another party. The criminal act is the attempt to deceive and attempted fraud is therefore treated as seriously as accomplished fraud.

- 2.3 Computer fraud is where information technology equipment has been used to manipulate programs or data dishonestly or where an IT system was a material factor in the perpetration of a fraud.

3.0 TRUST POSITION ON FRAUD

- 3.1 The Trust Board is absolutely committed to maintaining an anti-fraud culture in the organisation so that all staff who work in the Trust are aware of the risk of fraud, of what constitutes a fraud and the procedures for reporting it. The Trust adopts a zero-tolerance approach to fraud and will not accept any level of fraud within the organisation. It is also Trust policy that there will be a thorough investigation of all allegations or suspicions of fraud and robust action will be taken where fraud is proven in line with the Trust's Fraud Response Plan.
- 3.2 The Trust Board wishes to encourage anyone having reasonable suspicions of fraud to report them. It is the policy of this Trust, which will be rigorously enforced, that no employee will suffer in any way as a result of reporting reasonably held suspicions of fraud. For these purposes "reasonably held suspicions" shall mean any suspicions other than those that are raised maliciously. Further guidance on the protection afforded to staff is contained in the Trust's policy on Whistle Blowing.
- 3.3 The Trust Board will, however, take a serious view of allegations against staff that are malicious in nature and anyone making such an allegation may be subject to disciplinary action.
- 3.4 After proper investigation of any allegation or suspicion of fraud, in line with the Trust's Fraud Response Plan, the Trust will consider the most appropriate action or actions to take. Where fraud involving a Trust employee is proven, the Trust will instigate disciplinary action against the employee which may result in dismissal.
- 3.5 Where a fraud is proven, whether involving an employee or an external party, the Trust will, in conjunction with the Business Services Organisation (BSO) Counter Fraud and Probity Services (CFPS) Team, report the matter to the PSNI with a view to pursuing a criminal prosecution. The Trust will also seek to recover all losses resulting from the fraud, if necessary through civil court proceedings.
- 3.6 The Trust has adopted the DHPSS Counter Fraud Strategy as the basis for its anti-fraud activities. The key elements of this Strategy are as follows:
- The creation of an anti-fraud culture;
 - Maximum deterrence of fraud;
 - Successful prevention of fraud;
 - Prompt detection of fraud;
 - Professional investigation of suspected and detected fraud;

- Effective sanctions, including appropriate legal action against anyone found guilty of committing fraud;
- Effective methods for seeking recovery of money defrauded or imposition of other legal remedies.

4.0 FRAUD PREVENTION AND DETECTION

- 4.1 The Trust wholeheartedly supports the role of the BSO CFPS Team and will ensure that appropriate fraud prevention and detection measures are implemented in accordance with the CFPS guidance.
- 4.2 The Trust has implemented a range of policies and procedures that are designed to ensure probity, business integrity and minimise the likelihood and impact of incidents of fraud arising. The Trust has appointed a Fraud Liaison Officer (FLO) who takes the lead role for the Trust on all matters relating to fraud.
- 4.3 The Trust has also put in place a robust Internal Audit service that is actively involved in the review of the adequacy and effectiveness of control systems thereby further deterring the commissioning of fraud.

5.0 AVENUES FOR REPORTING

- 5.1 The Trust has a number of avenues by which staff can raise suspicions of fraud. These are detailed below and in the Trust’s Fraud Response Plan and Whistle Blowing Policy. Concerns should be raised initially with the appropriate line manager. However, staff can raise their concerns directly with their Director, the Director of Finance or the Head of Internal Audit if they so wish. Staff should also be aware that DHSSPS has in place a fraud reporting hotline that can be used to highlight concerns in confidence and anonymously if preferred. Alternatively, the Trust has a Policy & Procedure relating to Public Interest Disclosures (‘Whistleblowing’) which complements the Trusts Fraud Policy and Fraud Response Plan. Within this policy, the Trust has appointed a Delegated Person as the initial point of contact for complaints under the formal procedure. The Designated Person will usually be a Non Executive Director of the Trust. If the complaint is of a financial nature (for example concerns regarding the improper use of public funds) then the Designated Person will have direct access to the chair of the Trust’s Audit Committee. All information will be treated in the strictest confidence. The relevant contact details are as follows:

Director of Finance	028 9040 0751
Head of Internal Audit	0300 5550115
DHSSPS Fraud Hotline	0800 0963396
Designated Person (Whistleblowing)	028 9040 0713

- 5.2 If staff are unsure whether or how to raise a concern or want confidential advice at any stage, they may contact their union. They may also contact the independent charity Public Concern at Work on 020 7404 6609 or by email at helpline@pcaw.co.uk. Their legal team can talk staff through their options and

help them to raise a concern about malpractice at work. For more information, visit the website at www.pcaw.co.uk.

6.0 CONCLUSION

6.1 Whilst the individual circumstances surrounding each fraud will vary, the Trust takes all cases very seriously and adopts a zero-tolerance approach. All reported suspicions will be fully investigated and robust action will be taken where fraud can be proven.

7.0 EQUALITY STATEMENT

7.1 In line with duties under Section 75 of the Northern Ireland Act 1998; Targeting Social Need Initiative; Disability Discrimination Act 1995 and the Human Rights Act 1998, an initial screening exercise, to ascertain if this policy should be subject to a full impact assessment, has been carried out.

7.2 The outcome of the screening exercise for this policy is:

Major impact
Minor impact
No impact.

8.0 SIGNATORIES

_____ Date: _____
Lead Author

_____ Date: _____
Lead Director

Review of Policy

This policy will be reviewed every three years or at times considered necessary as a result of operational changes, legislative changes or risk assessments have occurred.

Date of Issue: June 2016
Date for Review: May 2019