FRAUD PREVENTION & RESPONSE PLAN

Introduction

The objective of the Fraud Prevention and Response Plan is to safeguard the proper use of the University's finances and resources, including the finances and resources of its subsidiary companies, against fraudulent acts, and to comply with the law and relevant regulations.

The University which derives a significant proportion of its income from public funds, benefactions and charitable organisations, has a particular responsibility to ensure that income and resources are used solely for the purposes intended.

Definitions

Fraud can be defined as including any of the following and other regulations that may cover other areas of fraud:

- Theft
- False accounting
- Bribery
- Corruption
- Money laundering
- Forgery
- Deception and collusion
- Other financial malpractice

For the purposes of reporting fraud the University considers a person acts fraudulently when he or she acts with the intent of making a financial gain or causing a financial loss or exposing another to the risk of financial loss.

This includes:

Dishonestly makes a false representation, or

Dishonestly fails to disclose information which he or she is under a legal duty to disclose; or

Occupies a position in which he/she is expected to safeguard, or not to act against, the financial interests of another person and;

Dishonestly abuses that position; and

Intend, by means of the abuse of the position:

POLICY

Authors: Lorraine Loy
Approved By: PME
Date: 23 October 2008
Version: 4

(a) to make a gain for himself/herself or another

or

(b) to cause loss to another or to expose another to risk of loss

Any person may be regarded as having abused his/her position even though his/her conduct consisted of an omission rather than an act.

Policy

Fraud is a serious matter and all cases of suspected fraud will be investigated, whether they concern the assets of the University, or of persons or bodies connected with the University. Any student and/or member of staff, regardless of their position or seniority, against whom prima facie evidence of fraud is found, will be subject to disciplinary procedures which may result in dismissal or summary dismissal.

The University reserves the right to seek redress via civil proceedings against individuals whose fraudulent acts have resulted in financial or other loss to the University, whether or not the individual concerned is criminally convicted of that fraudulent act.

The University may involve the police in any case of fraud or suspected fraud at any stage of an investigation.

The University will inform the relevant grant funding body in accordance with the terms and conditions of the grant in any case where the allegation may concern abuse of funds or assets of that body.

The University financial regulations, which apply to the conduct of all the financial affairs of the University, apply to all members of staff.

The regulations govern the proper use of finances and resources which may for example, involve cash, equipment, facilities, information, staff time, physical or intellectual property in a manner which satisfies the University's requirement for accountability, internal control, and the management of financial risk including any legal or financial obligations laid down by HM Revenue and Customs, the funding council and other government authorities. The University's financial regulations can be viewed at http://www.hw.ac.uk/reference/financial/regulations.pdf

What do you do if you think there might be fraud?

Any member of staff who suspects fraud with good cause that fraud has been committed must report the matter to the Secretary of the University immediately. A separate paper "Preventing Fraud – Guidance for Managers" sets out guidance for managers and supervisors on their role in preventing fraud.

If the Secretary of the University is suspected of fraud, the matter should be reported to the Principal & Vice-Chancellor.

The Secretary of the University will respond to the reported fraud in accordance with the Fraud Response plan.

All reports of suspected fraud will be treated in the strictest confidence, and any investigation under the procedure will be treated as an investigation under the University's Public Disclosure Policy. www.hw.ac.uk/hr

POLICY

In order to maintain confidentiality, and prevent compromising any related investigations, employees who are aware of any circumstances of fraud should not discuss those circumstances with other members of staff or with any other person other than those directly involved in the investigation.

Any individual who makes a report of suspected fraud will be protected under the provision of the University's Public Disclosure Policy (whistle blowers charter) if the report is made in good faith.

Fraud Prevention

The aftermath of fraud is costly, time-consuming, disruptive and unpleasant. The major thrust of any anti-fraud strategy should therefore be prevention. Measures that the University can put in place include denial of opportunity, effective leadership, auditing, and employee screening.

POLICY

FRAUD RESPONSE PLAN

Purpose and Scope

1. Management and staff are likely to have little experience in dealing with fraud and, when suspected cases arise, may be unsure of the appropriate action to take. The purpose of the Fraud Response plan is to document the procedures in the event of reported or suspected fraud or irregularity, together with defining authority levels, responsibilities for action, and reporting lines. The objective is to safeguard the proper use of the University's finances and resources, including those of its subsidiary companies and to protect the University's reputation.

2. The purpose for establishing this plan is so that the University is able to respond appropriately if the need arises; it is not a reflection on the probity of any member of the University.

3. The use of the plan should enable the University to:

   - prevent further loss
   - establish and secure evidence necessary for disciplinary and criminal action
   - assign responsibility for investigating the incident
   - establish circumstances in which external specialists should be involved
   - establish lines of communication with the police
   - keep all staff with a need to know suitably informed about the incident and the University's response
   - recover losses
   - deal with requests for references for employees and students disciplined, dismissed or prosecuted for fraud
   - review the reasons for the incident, the measures taken to prevent a recurrence, and any action needed to strengthen future responses to fraud.

4. The procedures set out in this plan apply to members of Court, members of staff employed by the University, temporary members of staff, contractors and students. These procedures also cover incidents that involve the alleged misuse of information or actions that impair the integrity of the assessment process arising from corrupt practices.

Initiating action

5. Suspicion of fraud or irregularity may be captured through a number of means, including the following:

   - the operation of proper procedures
   - the requirement on all staff under the Financial Regulations to report fraud or irregularity to the Secretary of the University
   - the public disclosure policy ('whistle-blower's charter')

POLICY

- planned audit work
- the University's policy on conflict of interest

Notification of suspected fraud

6. All actual or suspected incidents are reportable immediately to the Secretary of the University. There are special arrangements for the Principal & Vice-Chancellor, Vice-Principal, Deputy Principal for Strategy and Resources, the Director of Finance, the Management & Financial Accountants, and members of Court, which are set out below.

7. The Secretary of the University will determine whether to investigate a suspected incident under the University's Disciplinary Procedure or this Fraud Response Plan. Normally, the Secretary of the University will determine that an investigation will take place under the University's Disciplinary Procedure for 'minor' losses or infringements, and the Fraud Response Plan will be used for 'major' suspected wrong doing.

8. If the investigation of an incident is to take place under the Fraud Response Plan, the Secretary of the University will decide on the initial response and take such steps as are necessary to:

   - Prevent further loss/damage
   - Establish and secure evidence
   - Notify the necessary individuals, committees, and outside authorities
   - Recover any loss

9. A Fraud Response Group will support the Secretary of the University, and may include as relevant:

   - Deputy Principal for Strategy and Resources
   - A solicitor recommended by the legal advisor
   - Director of Finance
   - Group Management Accountant (where necessary)
   - Group Financial Accountant (where necessary)
   - Director of Human Resources (where relevant)
   - Academic Registrar and Deputy Secretary (where relevant)

10. The Secretary of the University will determine how the Fraud Response Group will operate. This includes individual consultation as well as face-to-face meetings of all members of the group.

11. To ensure speedy action, the Secretary of the University and Director of Finance may consult members of the Fraud Response Group individually. The Fraud Response Group will advise the Secretary of the University and the Director of Finance on the necessary measures to enable the formulation of a plan of action. This will normally include an investigation, led by the Secretary of the University.

12. The decision to initiate an investigation shall constitute sufficient authority to any person, authorised by the Secretary of the University, to conduct, in whole or in part, an investigation for this purpose.

13. The Secretary of the University may invite the internal or external auditors to lead the investigation, as the circumstances require. This will depend on the severity of the suspected fraud.

14. In cases that involve or may involve students and financial fraud, and which are initially identified by the University Finance Office, the Secretary of the University will be informed by the Director of Finance at an early stage.

15. The Secretary of the University will inform other relevant members of staff, at an early stage including the Principal, Vice-Chancellor and Vice- Principal, Director of UICS and the Director of Corporate Communications.

16. The University Solicitor will notify the Group Risk Manager at an early stage, to ensure the prompt addressing of insurance matters. The University Solicitor will seek expert legal advice, if considered appropriate by the Secretary of the University.

17. There will be an immediate report made by the Secretary of the University to the internal auditors of more serious, or novel, cases of fraud.

Notification of suspected fraud involving the Secretary of the University, Director of Finance and Deputy Directors of Finance

18. All actual or suspected incidents that concern the Secretary of the University, Director of Finance, the Management/Financial Accountants are reportable immediately to the Principal & Vice-Chancellor. In allegations that concern the above members of staff the investigation will be led by the Principal & Vice-Chancellor, following the procedures outlined above. In all such cases, the internal auditors will be informed immediately and commissioned to carry out the investigation into the allegations.

Notification of suspected fraud involving the Principal & Vice-Chancellor

19. All actual or suspected incidents that concern the Principal & Vice-Chancellor are reportable immediately to the Chairman of Court and the investigation will be led by the Chairman of Court. The internal auditors will be commissioned to carry out any investigation into the allegations concerning the Principal & Vice-Chancellor.

Notification of suspected fraud involving a member of Court

20. All actual or suspected incidents that concern a member of Court are reportable immediately to the Chancellor (Chair of the Board of Governors). In allegations that concern a member of Court, the investigation will be led by the Chancellor.

Notification of suspected fraud involving the Chancellor

21. All actual or suspected incidents that concern the Chancellor are reportable immediately to the Principal & Vice-Chancellor and to the Chairman of Court. In allegations that concern the Chancellor, the investigation will be led by the Chairman of Court. The internal auditors will be instructed to carry out any investigation into the allegations concerning the Chancellor.

Prevention of further loss

22. Where initial investigation provides reasonable grounds for suspecting an individual, or a group of individuals, of fraud, the Secretary of the University will decide how to prevent further loss/damage, taking advice from the Fraud Response Group. This may include suspension of

members of staff under suspicion, in accordance with University procedures. Where appropriate, it may be necessary to take similar action in the case of students, contractors or temporary members of staff. It may be necessary to plan the timing of suspension to prevent the suspects from destroying or removing evidence that may be required to support disciplinary or criminal action.

23. If a suspect is aware that an investigation is in progress, there may be an attempt to frustrate disciplinary or legal action by destroying or removing evidence. Therefore, it is vital to approach unannounced the suspect(s), who should be kept under supervision at all times before leaving the University's premises. The suspect(s) may collect personal property under supervision, but should not be able to remove any property belonging to the University. The suspect(s) will be asked to return any keys and or swipe cards to the premises, offices and furniture. The University Security Manager will supervise this process.

24. The University Security Manager will advise, through seeking advice, on the best means of denying access to the University, while suspect(s) remain suspended, for example by changing locks and informing the Security Patrol Officers not to admit the individuals to any part of the premises. Similarly, the Director of UICS is to arrange for the immediate withdrawal of access permissions to the University's computer systems. This is to include cancellation of all passwords to University databases and other information systems.

25. The Secretary of the University shall consider whether it is necessary to investigate systems other than those which have given rise to suspicion, through which the suspect(s) may have had opportunities to misappropriate the University's assets.

Establishing and securing evidence

26. The major objectives in any fraud investigation will be the punishment of the perpetrators, and for the process to act as a deterrent and to protect the University's reputation. The University will follow the disciplinary procedures against any member of staff or student who has committed fraud.

27. The University will normally pursue the prosecution of any such individual. Prosecution is a particularly effective deterrent because of the risk of a custodial sentence and a criminal record. However, the threat of prosecution only deters if the threat is real. Therefore, each case arising will normally result in reference to the police, irrespective of the status of the individual following legal advice.

The Secretary of the University will:

28. Maintain familiarity with the University's disciplinary procedures, to ensure that evidence requirements will be met during any fraud investigation following consultation with the Principal & Vice-Chancellor, or in the absence of the Principal & Vice-Chancellor the Vice-Principal or University Solicitor.

29. Establish and maintain contact with the police. Ensure that staff involved in fraud investigations are familiar with and follow rules on the admissibility of documentary and other evidence in criminal proceedings.

30. To be admissible in court, interviews with suspects must be conducted under rules defined in the Police and Criminal Evidence Act, 1984. Interviews should normally be conducted by Police Officers or with University advice. The Secretary of the University will establish whether there is a need for staff involved, or likely to be involved, with investigation to be trained in the evidence rules for interviews under the Police and Criminal Evidence Act, 1984.

POLICY

Recovery of losses

31. Recovering financial losses is a major objective of any fraud investigation. The Director of Finance shall ensure that, in all fraud investigations, there is the quantification of the amount of any loss. The University will seek the repayment of losses in all cases.

32. Where the loss is substantial, the University Solicitor will immediately obtain legal advice about the need to freeze the suspect's assets, through the court, pending conclusion of the investigation. The University Solicitor will also seek legal advice about prospects for recovering losses through the civil court, where the perpetrator refuses repayment. The University would normally expect to recover costs in addition to losses.

References for employees and students disciplined or prosecuted for fraud

33. Any request for a reference for a member of staff disciplined, or prosecuted, for fraud must be referred to the Director of Human Resources. The Director of Human Resources will consult with the University Solicitor and the Data Protection Officer to ensure that any reference accords with employment law principles.

34. Any request for a reference for a student or graduate disciplined or prosecuted for fraud must be referred to the Academic Registrar and Deputy Secretary. The Academic Registrar and Deputy Secretary will consult with the University Solicitor and Data Protection Officer to ensure that nay reference accords with employment law principles.

Reporting financial fraud to the Audit Committees

35. The Secretary of the University shall report any incident to the Chair of the Finance and Audit Committees.

36. The Secretary of the University shall promptly report any significant variation from the approved fraud response plan, together with reasons for the variation, to the chair of both the Finance and the Audit Committee.

37. On completion of a special investigation, a written report shall be submitted to the Audit Committee containing:

    - A description of the incident, including the value of any loss, the people involved, and the means of perpetrating the fraud
    - The measures taken to prevent a recurrence
    - Any action needed to strengthen future responses to fraud, with a follow-up report on the actions taken.

    The Director of Finance will normally prepare this report.

Reporting lines

38. The Fraud Response Group shall provide a confidential report to the Chairman of Court and the Chairman of the Audit Committee, external audit and the Director of Corporate Communications at least monthly, unless the report recipients request a lesser frequency. The scope of the report shall include:

    - quantification of losses/damage
    - progress with recovery action
    - progress with disciplinary action

- progress with criminal action
- estimate of resources required to conclude the investigation
- actions taken to prevent and detect similar incidents.

39. The individual(s) under investigation will be informed of the outcome, when the report has been completed.

Responsibility for investigation

40. The Secretary of the University shall normally lead all special investigations. Where appropriate, the Secretary of the University may delegate the conduct of the investigation to the Director of Finance or other staff.
41. In undertaking any investigation under the Fraud Response Plan, the investigation will follow those principles and procedures detailed in the University's disciplinary procedures.

42. Those charged with the investigation will have unrestricted right of access to all vouchers, documents, accounts, computer data, and any other information considered relevant to the investigation, and which is necessary to complete the enquiries. This includes the right to verify assets and have direct access to any employee or person responsible for the administration or management of University resources with whom it is felt necessary to raise and discuss such matters. All managers are required to co-operate with requests for assistance in respect of any investigation.

43. All investigations shall be completed in a timely manner.

44. Some special investigations may require the use of technical expertise that the University does not possess. In these circumstances, the Fraud Response Group may approve the appointment of external specialists to lead or contribute to the special investigation.

45. Any disciplinary action arising from the investigation will follow the procedures set out in the appropriate University disciplinary procedures.

Review of fraud response plan

46. There will be a review of this plan by the Secretary of the University and Director of Finance for fitness of purpose at least annually, or after each use. The audit committee will approve any change to the plan, with the exception of changes of office title included in the plan and minor changes of procedure.

POLICY

POLICY SUPPORT PAPER

MANAGING THE RISK OF FRAUD

Risk and Controls in Specific Systems

Purpose of the Paper

The purpose of this paper is to provide guidance to managers and supervisors on controls that must be in place in relevant processes. The document is structured so as to identify the risks associated with those areas with the greatest potential for fraud, with a particular focus on financial matters. The University has a number of existing controls which prevent the risk of fraud and reference should be made to the relevant policies, regulations and procedures referred to in the fraud response plan and guidance for managers.

This objective of this paper is to highlight some examples of where there is a potential for fraud to be committed and provides examples (not an exhaustive list) of the types of controls that must be incorporated across all aspects of University business.

Controls must be appropriate to the scale of the assets at risk and the potential loss to the University.

Risk associated with cash handling

There are many risks associated with cash handling. Theft or misappropriation of cash may be assisted by the suppression, falsification or destruction of accounting records, or where no initial records are created at all.

How fraud could be committed	Examples of controls
Theft	• Cash should be held securely at all times • Access to cash should be restricted to named personnel • Controls over keys should be set up and keys should only be issued to authorised staff • Cash balances should be kept to a minimum, recorded and checked periodically
Income received not recorded	• Always issue pre-numbered receipts • Maintain accurate records of income received • Post opening duties should be carried out by at least two people and a receipts log completed and signed by both officers where relevant. • Separate duties at key stages of the process: o post opening and logging of receipts; o recording receipts and preparation of cash and cheques for banking; o daily cash balancing and bank reconciliations • Regular and random management checks of source documentation, accounting records and bank reconciliations; • Rotation of staff
Illegal transfer or diversion of money Changes and additions to payee details through BACS	• Changes and additions to payee details and other standing data should be independently authorised • System access to make and authorise these changes should be carefully restricted and logged • Provide adequate supervision of all staff particularly new, inexperienced or temporary staff

	• All payments should be independently authorised before they are made • Restrict knowledge of passwords if payments are initiated by computer) to approved personnel. Passwords should be changed frequently and always when staff leave • Payment reports should be independently reviewed for accuracy immediately before the transfer of funds occurs • Separation of duties between those setting up payment accounts and those authorised to trigger payments should be maintained at all times. Similarly separate duties of receiving goods and services from the process of making payment
False creation of or unauthorised updates to accounting records to allow the unauthorised payment of funds	• Amendments and deletions to accounting records should be independently authorised. These should be evidenced by signature, together with name and grade • Independent checks to ensure amendments have been carried out correctly. These should be evidenced by signature, together with name and grade • Authorisation levels and frequency of checks, including the use of spot checks, should depend on: o the amounts involved; o the degree of risk associated with the system • Accounting records and petty cash should be reconciled on a regular basis. These reconciliations should be recorded and independently reviewed. Discrepancies should be investigated and resolved • Any discrepancies that cannot be resolved, or any losses that have occurred should be reported as part of a formally defined process • Suspense accounts should be reviewed on a regular basis to confirm their validity
Falsification and duplication of invoices in order to generate a false payment	• There should be segregation of duties between ordering and payment of invoices • Checks for duplicate invoices should be carried out periodically • Invoices should be checked back to orders for evidence that the orders were genuine and properly authorised and goods and services were received.
Unauthorised use of cheques and payable orders	• Financial stationery should be held securely and records kept of stock holdings, withdrawals and destruction of wasted stationery • Signatories and delegated powers should be established for cheques and payable orders • Cheques and payable order should be checked to source documentation before use • Use restrictive crossings such as “non-transferable” and “a/c payee” • Ensure that addresses to which payable instruments are sent are correct. For large value payments check encashment to ensure that the intended recipient did receive the payment • Discourage the fraudulent amendment of cheque details by careful choice of inks and printers so that the print produced on cheques is as indelible as possible • Print the amount in figures as close the £ sign as possible • Write payee details in full rather than use abbreviations or

	acronyms • Fill up blank spaces with insignificant characters such as asterisks • Use envelopes that make it less obvious that they contain cheques for mailing purposes • Ensure that signed cheques are not returned to payment staff • Reconcile bank statements with cheque listings regularly

This section provides some examples of controls relating to travel and subsistence that must be in place.

How fraud could be committed	Examples of controls
Making false claims for allowances, travel and subsistence.	• All staff are required to comply with the University's Financial Regulations • Establish a formal process that involves line managers approving and reviewing work plans and programmes for business trips. • checks by authorised signatories of claims against approved travel plans, standard mileages for regular destinations and primary evidence such as hotel bills, rail tickets and taxi receipts. • All amendments to details on claim forms must be initialled by the budget holder. Finance Office to reject any claims where amendments have not been initialled. • Budget holders/Financial Controllers to ensure that correct rates are claimed, sustaining documents (e.g. hotel invoices) are included and to compare counter signatures on claims against sample signatures provided by authorised authorised signatories. • Random management checks should be carried out to verify details on claims and to ensure that finance team checks are applied rigorously to claims. • Budget holders should be provided with sufficient information to enable them to monitor travel costs against budget.

Risks associated with research grants and contracts

This section sets out examples of the controls that should be in place to counter the fraud risks specifically associated with payment of grants:

How fraud could be committed	Examples of controls
Grant funds are misappropriated.	• All staff are required to comply with the Policy Statement on Research Grants and Contracts. • Guidelines on the claims procedures must be complied with and communicated to all staff employed to process claims. • Delegated authorities and levels of authorisation should be established. • Claims should be assessed to determine their complexity and level of risk and allocated accordingly by budget holders and financial controllers with the relevant experience and expertise. • All claims and supporting evidence should be checked for accuracy, completeness and timeliness.

POLICY

	• No single officer should be involved in processing and authorising a complete claim and appropriate segregation should be maintained throughout the process. • Good quality records should be maintained. • An officer with the appropriate delegated authority should give the final approval for a claim. • Training needs should be assessed periodically and appropriate training plans drawn up. • All claims relating to an individual or organisation should be identified and cross-referenced to reduce the risk of duplicating payments. • Periodic reassessments should be carried out where on-going claims are concerned. • Copies of all outgoing correspondence should be traceable to the originating officer. • Reports of research and consultancy payments should be regularly scrutinised to ensure that only approved grants/consultancy have been paid out and that they have gone to the correct recipients.

Risk associated with procurement

Risks associated with the operation of purchasing systems include the false input of invoices, the diversion of payments and misappropriation of purchases. This section sets out some examples of controls that should be in place to reduce the risk of fraud in this area:

How fraud could be committed	Examples of controls
Unauthorised use of purchasing systems in order to misappropriate goods or use services for personal gain.	• All staff are required to comply with University Financial Regulations and Procurement Policies & Procedures. • Restrict opportunity to generate payment by using sequentially numbered purchase order forms for all orders; perform independent checks to show that purchase orders are valid and accounted for. • Authorised signatories and their authorisation limits must be established for requisitioning and placing orders and adhered to. • Invoices must be authorised and matched to orders before the invoice is certified for payment. • Stock records must be maintained up to date so that stocks, stock usage and orders can be monitored. • There must be separation of duties between those ordering, receiving goods, and approving and paying invoices. This separation of duties should be reviewed regularly. • Authorised staff must only make amendments to standing data such as the supplier records. • Budget holders should regularly check items of expenditure charged against their budgets. • Regular and random management checks should be carried out to confirm the existence of assets.
Short deliveries of goods or services may be accepted as a result of collusion.	• Random management checks that involve matching copy orders to delivery notes and goods should be carried out.
Acceptance of unsolicited goods or expanded orders as a result of fraudulent acceptance	• Payment for goods should only be made after confirming that goods were properly ordered and authorised.

POLICY

of attractions such as free gifts.	
Misuse of Procurement Cards / Credit Cards	• All staff are required to comply with Procurement Policy Guidance with regard to University purchasing cards • Named individual should be appointed as cardholders. • All purchases should be approved by the budget holder. • Use suppliers with whom the University has a contractual relationship or is otherwise a reputable supplier. • Procurement Services distributes the cards agreed with the School, Institute or Section. The cardholder should sign the card in the presence of another staff member. The School, Institute or Section should maintain an up to date list of all its cardholders. • Cards should be returned to the Financial Controller when card holders move or cease to be cardholders. The Financial Controller must ensure that the card is destroyed and the record of cardholders amended. • Cardholders should hold cards securely. • Cardholders should check all entries on statements supplied by the bank and refer any discrepancies to the Financial Controller. • Budget holders should carry out periodic checks to ensure that card statements are properly reconciled and that only authorised purchases are made.
Orders placed on the internet fail to be delivered or goods received are not of desired quality.	• Make sure your browser is set to the highest level of security notification and monitoring. • Check that you are using the most up to date version of your browser and ensure their security features are activated. • Keep a record of the retailer's contact details, including a street address and non-mobile telephone number. Beware if these details are not available on the website. Do not rely on the email address alone. • Click on the security icon to see if the retailer has an encryption certificate. This should explain the type and extent of security and encryption it uses. Only use companies that have an encryption certificate and use secure transaction technology. • If you have any queries or concerns, telephone the company before giving them your card details to reassure yourself that the company is legitimate. • Print out your order and consider keeping copies of the retailer's terms and conditions and returns policy. Be aware that there may be additional charges such as postage and VAT, particularly if you are purchasing goods from traders abroad. When buying from overseas always err on the side of caution and remember that it may be difficult to seek redress if problems arise. • Check statements from the bank or card issuers carefully as soon as your receive them. Raise any discrepancies with the retailer concerned in the first instance. If you find any transaction on your statement that you are certain you did not make, contact your card issuer immediately. • Check that you are fully aware of any payment commitments you are entering into, including whether you are instructing a single payment or a series of payments. • Never disclose your card's PIN to anyone, including people

	claiming to be from you bank or the Police, and NEVER write it down or send it over the Internet. • If you have any doubts about giving your card details, use another method of payment.

Risks associated with the use of contractors

This section sets out some example of controls which should be in place, in addition to those which apply generally to cash handling and purchasing systems, to counter the fraud risks faced in relation to the use of contractors:

How fraud could be committed	Example of controls
A contractor could be selected as a result of favouritism or who does not offer best value for money.	• All staff are required to comply with the Procurement Policies and Procedures. • Draw up and agree a clear and comprehensive specification and tender documentation. • Seek tenders from suitable suppliers. • Tenders should be delivered to those responsible for selection without interference. • Late and/or qualified tenders must not be accepted. • Tenders should be evaluated by a tender evaluation panel against the agreed evaluation criteria. • The tender that offers the best value for money should be recommended for acceptance. • The Project Board and/or tender panel should approve the successful contractor. • Staff should be required to declare any personal interests they may have which may affect the tendering process.
Payments made for work not carried result out as a result of collusion between the contractor and official.	• Invoices are paid only when work or services have been satisfactorily carried out. • There is a register of contracts in progress. • Contractors are only added to the approved contractors list when properly approved and authorised. • Invoices are only accepted from approved contractors. • All contract variations are authorised, documented, variation orders are sequentially numbered, produced in an agreed format and authorised before payment. • Checks are made against budget and planned expenditure prior to approval of payment (except where specific conditions require a different pre-approved approval (e.g.) Architects Certificates.

Risks associated with assets

Risks in this area include use of assets for personal gain, or misappropriation of assets. This section suggests some controls that should be in place to counter those risks.

How fraud could be committed	Examples of controls
Theft or unauthorised use of assets.	• Asset register to be maintained up to date. Inventories to be used, where possible, and assets assigned to individual budget holders. • There is adequate definition of assets on the asset register. • Asset marking to be carried out where possible. • Physical security of assets to be maintained. • Spot checks on existence of assets to be carried out on a

POLICY

	regular basis.

Risks associated with sensitive information

The final section deals with some of the controls that should be in place to reduce the threat of fraud or other irregularities arising from access to sensitive information or misuse of information for private gain.

How fraud could be committed	Examples of control
Theft of sensitive / restricted documentation or information.	• All data should be stored securely and adequately backed up. • Personal data should be held in accordance with the Data Protection Act 1998 (e.g. fairly and lawfully processed; processed for specific purposes; not excessive; accurate; not held for longer than necessary; processed in line with data subject's rights; secure; not excessive, not transferred to countries where the rights of data subjects cannot be adequately protected). • Procedures should be in place to provide data subjects with access to data held about them in compliance with the Freedom of Information Act, and Human Rights Act). • Access to computer records should be restricted and if the system resets, logged and spot checks made to confirm that there were valid reasons for any unusual accesses. • Computer logs should be adequately protected against unauthorised access and amendment. • Staff should ensure they protect information being sent externally by ensuring electronic files are protected by converting files to pdf format or are password protected.

POLICY SUPPORT PAPER

PREVENTING FRAUD - GUIDANCE FOR MANAGERS

Introduction

The purpose of this paper is to provide guidance for managers and supervisors on their role in preventing fraud. It must be read in conjunction with the Fraud Prevention and Response plan.

This guidance must be drawn to the attention of relevant members of staff for whom the manager or supervisor is responsible.

The guidance in this paper applies equally when fraud is perpetrated (a) to gain an advantage from an outside body or individual, even if for the benefit of the University, and (b) to the receiving of inducements. An example of where fraud is perpetrated to gain an advantage from an outsider might be the offer of a bribe in order to gain a contract, which may be for the benefit of the University, but which is unacceptable behavior.

This guidance also extends to cases concerning students when this involves the University.

Prevention

1. The aftermath of fraud is costly, time-consuming, disruptive and unpleasant. The major thrust of any anti-fraud strategy must therefore be prevention. Measures that managers and supervisors in the University can put in place include denial of opportunity, effective leadership, auditing, and employee screening.

Denial of opportunity

2. Fraud can be minimised through compliance with University internal control systems and carefully designed and consistently operated management procedures, which deny opportunities for fraud. Managers must ensure that members of staff receive appropriate training in the operation of these systems. University financial regulations can be viewed at http://www.hw.ac.uk/reference/financial/regulations.pdf
3. It is possible to guard against fraud in financial systems through the separation of duties, so that no one individual has a disproportionate responsibility for either the management or administration of payments, income or assets. Where possible, staff must not have uncontrolled access to assets, if they have uncontrolled access to the records where these assets are recorded. Where appropriate, it may be possible to reduce any residual risk through periodically rotating staff that have access to financial systems. Computing Regulations can be viewed at www.hw.ac.uk/uics.

4. Managers must prevent the possible misuse of information technology through managing the physical access to terminals, and protecting systems with electronic access restrictions. This may need reinforcing through the importance of maintaining these control systems. www.hw.ac.uk/uics

Leadership

5. Key determinants of the standards of behavior will be the standards portrayed by managers, the practicality of the policies guiding action and managements approach to their enforcement.

6. To support managers in the promotion of public service values, the University has adopted and disseminated policies on;

    - the registration and declaration of interests by Governors and members of the management group http://www.hw.ac.uk/reference/financial/regulations.pdf

- the acceptance of hospitality and gifts
  http://www.hw.ac.uk/reference/financial/regulations.pdf

- the response in the event of a suspected fraud or irregularity http://www.hw.ac.uk/fraud

The role of auditors

7. When new systems are being designed or existing systems are to be modified, auditors can advise management on building in ways of preventing or detecting fraud.

8. A rolling review of systems by internal audit may deter attempted fraud and must result in continuous improvements. The risk of fraud will be a factor considered by external and internal auditors when designing audit plans. External audit's reviews of financial checks and balances and validation testing provide further deterrence, and may result in recommendation to improve controls.

Employee screening

9. Potential new members of staff must be screened before appointment, particularly for posts with financial responsibility. For example;

   - references must cover a reasonable, continuous period

   - applicants must be asked to explain any gaps in employment

   - a reference from the current or last employer must be obtained

   - doubts about the contents of the reference must be resolved before confirming the appointment [Note: If this is done by telephone, a written record of the discussion must be made and signed by the person undertaking the enquiry.]
     http://www.hw.ac.uk/students/data_protection_policy.pdf

   - essential qualifications must be checked before making an offer of employment

10. The University has a policy on the employment of job applicants who are related to existing staff or governors. Recruitment procedures require applicants to declare any connections with existing staff. Members of recruitment panels are also required to declare such connections.

Detection

11. No system of preventative measures can guarantee that frauds will not occur. The University seeks to include detection measures to highlight irregular transactions and weakness in internal management systems.

12. Quality management systems represent the most important measure because the risk of processing an irregular transaction is minimised where there is a systematic review of every transaction. Opportunity for detection and prevention must be designed into all systems and applied consistently. This would include segregation of duties, reconciliation procedures, random checking of transactions and review of management accounting information, including exception reports.

13. Systems must identify transactions that have not followed normal procedures. However, deception may be used to make improper transactions appear legitimate. Therefore, a more general approach to capture suspicions identified through chance, exit interviews and tip-offs must complement the checking elements in each system.

Public disclosure ('whistle-blowing') policy

14. The University has established public disclosure policy, following the Public Interest Disclosure Act 1998. The purpose is to promote the highest standards of openness, probity and accountability, and employees receive legal protection against being dismissed or penalised because of disclosing a serious concern. These procedures guarantee that the University will investigate concerns expressed in good faith, without adverse consequences for the complainant. www.hw.ac.uk/hr

Role of auditors in detection

15. The first lines of defence against fraud are robust preventative measures by managers and supervisors, coupled with a sound system of checks and division of responsibilities. Managers and supervisors must regard auditors as secondary to the internal systems that are under their control.

16. Nonetheless, where there is an identified high risk of fraud, University auditors may use specialised knowledge and experience to identify fraudulent transactions. In individual cases where it is necessary to invite either the internal or the external auditors for advice, the Fraud Response Plan will operate. Where the University wishes to seek general advice, the Secretary of the University will make the request.

17. Given the sensitivity of fraud, there must be an effective two-way flow of information between internal and external audit.

Warning signs

18. Patterns of behavior among staff that might indicate a desire for concealment. The responsible manager must investigate these. Examples of such behaviour in staff could include:

- taking few holidays or a reluctance to take leave
- regularly working alone late or at weekends for no apparent reason
- resistance to delegation
- resentment of questions about work
- sudden changes in behavior
- unexplained wealth and sudden change in lifestyle
- new staff resigning quickly
- excessive replacement of documentation
- important documents being lost and replaced by photocopies
- suppliers/contractors/customers insisting on dealing with a particular member of staff
- cosy relationships with suppliers/contractors/customers
- a member of staff under stress without a heavy workload
- refusal of promotion or a refusal to rotate responsibilities

19. If there is an indication of addiction to drugs, alcohol or gambling, the manager must consult with the Director of Human Resources as early as possible. This is both for the welfare of the individual, including matters relating to health and safety at work, and to minimise the risks to the University, which might include fraud.

Investigation

20. Fraud or irregularity occurs unpredictably, in any part and at any level in an organisation. It frequently causes disruption that is out of proportion to the sums involved.

21. Once there is a suspicion of fraud, prompt action is needed to safeguard assets, recover losses and secure evidence for effective legal and disciplinary processes. Meeting these objectives, when the full facts of a case may be unknown, clearly requires contingency planning. There is provision made for this eventuality in the University's Fraud Response Plan http://www.hw.ac.uk/fraud

22. The Fraud Response Plan includes the required steps in the event of a need for investigation. The plan is necessary to reduce the risk of:

- inadequate communication, which results in delayed or inappropriate action;
- failure to react fast enough, so that further losses are incurred or the evidence required for successful recovery or prosecution is lost;
- adverse publicity which could affect confidence in the University ; and
- creation of an environment which, because it may be perceived as being ill-prepared, increases the risk of fraud.

Vulnerable areas

23. The three areas most vulnerable to fraud are cash handling, cheque handling and purchase ledger.

Cash

24. There have been many examples of frauds in many organisations involving involving thefts from cash boxes, cash registers and takings at bars, residences, catering outlets, vending machines, and from social funds. Management of cash must include the following;

- Segregation of duties - Systems must prevent one person from receiving, recording and banking cash. The system must incorporate additional supervisory management, and unannounced spot checks. Segregation of duties must continue during periods of leave or sickness absence.
- Reconciliation procedures - An independent record of cash received and banked may deter and detect fraud. Documents used in reconciliation processes, such as paying-in slips, must not be available to the officer responsible for banking. It may be possible to sustain a very large fraud over a period of years, despite reconciliation procedures, because the officer responsible for receiving and banking cash fraudulently alters paying-in slips to conceal thefts, before the commencement of reconciliation procedures.
- The issue of receipts in return for cash received, to provide an audit trail.
- Physical security, such as keypad controlled cashiers' offices and safes. It is essential to keep keys and access codes secure.

POLICY

- The regular banking of cash.

- The use of alternatives to cash, including vending cards, credit cards, cheques, direct debits, and standing orders.

Cheques

25. Cheques are often completed in ways that facilitate opportunist fraud; and organised criminals who falsify payee and value details using sophisticated techniques sometimes intercept cheques. Debtors may also be told to make cheques payable to a private account, possibly using an account name that is similar to the University's.

Preventative measures include:

- Physical security **-** Unused, completed and cancelled cheques must never be left unsecured. If cheques are destroyed, more than one officer must be present, and a record of the serial numbers must be maintained.

- Frequent bank reconciliations - Some frauds go undetected for long periods because accounts have not been reconciled promptly, or because discrepancies have not been fully investigated.

- Segregation of duties

- Use of bank account names that will be difficult to represent as personal names, to prevent the simple theft of cheques in the post and the University s conversion into cash.

- Clear instructions to debtors about correct payee details and the address to which cheques must be sent. The address must normally be the Finance Office, not the School, Institute or Section that has provided the goods or services.

- Central opening of all post by more than one person, and recording of all cash and cheques received.

- Rotation of staff responsibilities, including the regular rotation of counter-signatories, to reduce the risk of collusion.

- Training staff in the secure completion of cheques.

- Use of electronic funds transfer as an alternative to cheques.

- Occasional checks with local banks of accounts including the University's name would help identify accounts operated contrary to Financial Regulations, even for personal use.

Purchase ledger

26. Many of the largest frauds suffered by higher education institutions have targeted the purchase ledger.

Preventative measures include:

- Minimising little used or unusual account codes.

- Ensuring that line management effectively monitors all account codes.

- Segregation of duties.

POLICY

- Secure management of the creditors' standing data file, including segregating the origination and approval of new or amended data.
- Requiring purchase orders for the procurement of all services, as well as goods.
- The deployment of unsuitable employees away from purchasing.
- The vetting of all suppliers would help establish that they are genuine and reputable companies, before inclusion on the lists of authorised suppliers.

Commercial ethics

27. In all dealings with commercial partners, the interests of the University are paramount. It is vital that all members of staff avoid any personal or family gain or the perception of such gain. In this context, 'commercial partners' also extends to public bodies with whom the University is entering a contractual relationship.

28. Members of the University Court and the Planning & Management Executive are required to record any interest in writing on an annual basis. Members of University Court are required to declare an interest in the business of the meeting. The University's Conflict of Interest Policy is available at: www.hw.ac.uk/hr

29. It is vital to make clear to all suppliers and contractors that the University will not do business with companies that seek to circumvent the established procurement policies, or that offer inducements to University staff.

30. Where appropriate, an anti-corruption clause may be included in standard tender and contract documentation. This may act as an effective reminder to contractors, suppliers and University staff that selflessness is required in commercial relationships. The following is a model clause:

"You shall not give, provide, or offer to University staff and agents any loan, fee, reward, gift, except items of negligible intrinsic value, or any emolument or advantage whatsoever. In the event of any breach of this condition, the University shall be at liberty forthwith to terminate the contract and to recover from you any loss or damage resulting from such termination, without prejudice to any other rights we may possess".

Review of Guidance

This guidance is subject to periodic review, drawing on the experience of usage.

POLICY