Pearson plc: Code of Business Conduct
Whistle Blowing – Privacy Policy

1. **Objective –** to define the procedures and process to protect an employee's right to privacy and fair treatment with regard to the operation of the company's whistle blowing arrangements.

2. **Scope** – all Pearson businesses globally with the exception of:

   - **IDC** – who, as a NYSE quoted company, have their own code of business conduct and separate whistle blowing arrangements
   - **Joint Ventures**, e.g, The Economist, who maintain their own independent arrangements.

3. **Background**

   Pearson's Code of Business Conduct (the Code) sets out the behaviourial norms the company expects from its employees when conducting business, externally and internally, and carrying out their daily job responsibilities. Its aim is to ensure that Pearson conducts business on a legal and ethical basis, in all countries, and that employees are treated fairly. It also describes unacceptable behaviour.

   The Code is posted on the Pearson corporate website and intranet (www.pearson.com and www.pearsontopearson.com) as well as individual operating company (Opco) intranets. Opco senior management are responsible for ensuring the Code is circulated within their business and understood by their staff. Annually, employees are asked to confirm their awareness of the Code and to report any potential breaches in the Code they may be aware of.

   The Code also enables Pearson to comply with UK and US corporate governance requirements relating to the reporting of fraud, particularly those concerned with accounting, auditing and financial reporting matters. In particular it allows the company to comply with its obligations under the US Sarbanes-Oxley Act of 2002 (SOX).

4. **Reporting breaches in the Code – Operating Company**

   The section of the Code headed "Making sure we comply with the Code" describes the reporting procedures that employees should follow if they believe the Code is being breached.

   In the first instance they should report their concerns to their local Opco legal counsel, who will confidentially investigate their complaint. As part of any investigation, legal counsel will involve relevant management, including Human Resources (HR), and employees on a need to know basis. The conclusions of the investigation will be communicated to the employee and any necessary action, including disciplinary action as defined under the operating company's standard HR

policies and practices, will be taken as appropriate. Findings will be kept confidential and only reported to the following management:

- Local Opco senior management - CEO or equivalent, HR Director and relevant functional management on a needs to know basis
- Opco Regional Management – CEO or equivalent, HR Director and relevant functional management on a needs to know basis
- Pearson plc – Group Legal Counsel and Head of Group Control and Director of People and Pearson Management Committee (PMC) member responsible for the business/function

5. Reporting breaches in the Code – hotlines and online reporting systems

To complement existing Opco reporting systems in relation to the Code, Pearson has also established a free, confidential whistle blowing telephone hotline and online reporting system. Employees can use the hotline or the online reporting tool to report any concerns they may have about any behaviour that is inconsistent with the Code.

One of the purposes of the whistle blowing reporting systems is to enable Pearson to meet its obligations under SOX regarding the adoption of formal procedures, by the Audit Committee, for addressing complaints relating to fraud, accounting and auditing matters.

For local regulatory reasons, reports made via these reporting systems by employees based in certain European Union countries, or about incidents that took place in these countries, may be limited to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery including conflicts of interest, banking and financial crime. Other matters in these countries should be reported via the process set out in point 4 above.

To protect an individual employee's legal rights and privacy, the following procedures have been adopted:

5.1 Procedures for dealing with a complaint

On receipt of a complaint the Group Legal Counsel and Head of Group Internal Audit will consult on the steps to be taken. If appropriate, an investigation will be initiated based on the criteria described in 5.3 below. If no action is required, because the information provided is inadequate and/or unclear, the report will be archived, deleted or anonymised as appropriate.

Appropriate resources, internal and external, will be engaged on a need to know basis to assist with any investigation, which will be overseen by the Head of Group Internal Audit.

The results of the investigation will be reported back to the Head of Group Internal Audit and Group Legal Counsel and discussed with relevant individuals and Opco management on a need to know basis.

5.2 Protection of reported information

5.2.1 The Pearson Information Security policy (see http://intranet.pearsontc.com/index.cfm?a=cat&cid=844) defines the policies and procedures adopted by Pearson to secure all information, both in electronic and paper formats.

5.2.2 The whistle blowing reporting systems are managed by a third party, Ethicspoint, on Pearson's behalf and incorporate the strictest levels of security, confidentiality and standards, through a combination of best practices to protect systems using industry standards, including ISP 17799, CobiT and BS 7799. The role of Ethicspoint is to ***record complaints only***; all investigations are conducted by Pearson senior management as described elsewhere in this policy.

5.2.3 The Ethicspoint service is a secure system, located in the US. Ethicspoint is compliant with appropriate US, European Union and other international laws in relation to individual employee's rights under data privacy legislation.

5.2.4 Within Pearson, access to reported information is restricted (using strict password security) to the Group Legal Counsel, Head of Group Internal Audit and two designated Audit Managers within the Group Internal Audit function, one of whom acts as the system administrator and the other who is the EU Code of Conduct (COCO) Coordinator.

5.2.5 To comply with EU rules on the transfer of personal information outside of the EU, information reported by employees based in EU countries can only be accessed by the Group Legal Counsel, Head of Group Internal Audit and the Senior Audit Manager – EMA/Asia, who acts as the EU COCO Coordinator and is based in London.

5.2.6 For US complaints, HR type matters can be also be accessed directly by the US Senior VP Human Resources and two of his designated senior managers.

5.2.7 Where necessary, on a temporary basis only, selected managers may be given access to the Ethicspoint system by the Head of Group Internal Audit to assist in an investigation. This access is restricted solely to the complaint being investigated.

5.3 Investigation criteria

5.3.1 HR issues not involving alleged fraudulent activity and/or a serious breach in the Code will be passed back to local HR function to deal with under standard Opco HR policies and procedures.

5.3.2 Allegations of fraud (including conflicts of interest), accounting matters, internal accounting control, audit matters, bribery, banking and financial crime ("Qualifying Allegations") will be investigated via the Group Internal Audit function. The Head of Group Internal Audit will engage resources, internal and external, as deemed necessary on a need to know basis.

5.4 Reporting of allegations/investigations

5.4.1 HR issues – the matter will be dealt with locally under standard Opco HR polices and procedures. A detailed record of the complaint will be retained by Opco. Results of investigation will be reported as in point 4 above.

5.4.2 Qualifying Allegations – results of investigations will be reported to:

- Opco CEO and relevant senior management on a need to know basis
- Opco Regional Management – CEO or equivalent, HR Director and relevant functional management on a need to know basis
- PMC member responsible for the business
- Pearson Group CFO
- Audit Committee
- Pearson Group CEO and Director of People (where necessary)

5.5 Recordkeeping and document retention

5.5.1 A secure log of all whistle blowing allegations is maintained and accessed by Head of Group Internal Audit and authorized Audit Managers. The log is a simple record of:

- Individual's name (if given) making allegations
- Pearson unit
- Brief description of allegation
- Brief description of results of investigations
- Status of investigation, i.e. in-progress or closed

5.5.2 The log is maintained securely under the supervision of the Head of Group Internal Audit.

5.5.3 Paper copies of the log and relevant supporting documentation on completion of an investigation are securely maintained under the supervision of the Head of Internal Audit. Where appropriate local Opco management, usually HR, will also maintain a detailed hard copy record of the investigation.

5.5.4 Log and supporting documentation regarding investigations of Qualifying Allegations are maintained for a period up to 7 years where deemed necessary to provide evidence to relevant authorities and support any legal claims. Local Opcos will maintain all detailed records for HR issues as defined in 5.4.1 above.

5.5.5 Personal data relating to reports that are found to be entirely unsubstantiated will be deleted without delay where this is legally required, subject to legal or regulatory data retention requirements.

5.5.6 The PwC senior partner has supervised access to the log and Ethicspoint systems as part of annual external audit process.

5.6 Employee notification and communication

5.6.1 We encourage all employees to include their name and operating company when making a report to aid the investigation. The identity of all callers will be treated confidentially, unless otherwise legally required.

5.6.2 No action will be taken against any employee reporting actual or suspected wrongdoing.

5.6.3 Any use of the whistle blowing reporting systems for reporting of frivolous or defamatory allegations or for personal reasons is unacceptable. The making of such reports is in itself a breach of the Code and will be treated extremely seriously. Employees who make any such reports will be subject to disciplinary action under our standard HR policies.

5.6.4 Where required for legal reasons, employees that are the subject of a report will be notified as soon as appropriate that information is held about them, by whom and for what purpose. They will also be notified of their rights of access, and of rectification and erasure of incorrect information, and whom they should contact with queries. This notification to an employee will take place once it is decided that the notification would not jeopardise the company's ability to investigate the allegation.

5.7 Annual employee confirmation exercise

Employees are asked annually to confirm their awareness of the Code and report any known breaches in the Code they may be aware of. The confirmation is in the form of a simple yes/no questionnaire – no information on alleged breaches is asked for at this stage of the confirmation process. This exercise is overseen by the Head of Group Internal Audit.

Where an employee indicates they are aware of a breach they are contacted directly by the Head of Group Internal Audit (or his/her designated proxies) to

discuss the nature of the alleged breach. Depending on the allegations made the following steps will be taken:

- No action if allegation relates to a previously reported and resolved matter
- Local HR issue – follow procedures described in 4 above.
- Qualifying Allegations – follow procedures described in 5.3-5.6 above.

Bob Dancy
Pearson Group Legal Counsel
27 May 2008

Robert Harris
Head of Group Internal Audit
27 May 2008