

Guidance on handling sensitive data

The OFT receives a great deal of sensitive information during the course of its work; information which relates both to individuals and to businesses. It is vital the information received is handled with great care.

Specific legislation for handling information

The Enterprise Act prohibits the disclosure of any information which we have received during the course of our investigations. Information may nevertheless be disclosed in certain circumstances, provided that certain factors are satisfied. Any other disclosure is a criminal offence. We, therefore, need to be careful in every case that we have considered the Enterprise Act provisions before any disclosure is made.

The Official Secrets Act 1989 requires all civil servants to exercise care in the use of information acquired during official duties and to protect information which is held in confidence. We have all signed the Official Secrets Act. Breach of the provisions of the Official Secrets Act may in certain circumstances lead to criminal or civil proceedings.

Insider trading is a criminal offence. There are special provisions in relation to public servants in the Company Securities (Insider Dealing) Act 1985. Care must be taken in the use of unpublished sensitive information that is likely to affect the share price of particular companies. In particular, you must not deal in the securities of those companies nor work with others who do so.

The Data Protection Act covers personal data. The OFT needs to collect and use certain types of information about the people with whom it deals in order to operate. These include individuals who are being investigated; individuals who supply information or conduct business with the OFT, callers to Consumer Direct, the OFT's own employees, suppliers and others with whom the OFT conducts business. Care must be taken in handling personal data.

Practical steps

A practical step to ensuring that we are not inadvertently responsible for disclosure of information is to ensure that we all operate a clear desk policy. Only have the papers you are working on in front of you and make sure that you lock everything away when you leave the office. It is also important that you discuss sensitive work only with those who need to know what you are doing and only within the Office building, or if you are at an external location and discussion of the matter cannot wait your return to the Office, with due care to avoiding others picking up on the conversation.

If you have any queries about these issues you should speak to your manager. If you have any concerns about a specific disclosure of information, you should consult one of the following:

The Departmental Security Officer: Milton Watts

Director, Executive Office: Erik Wilson

Data Protection and Freedom of Information Coordinator: Ian Bennett

Computer Security: Luke McAuley