

1

GUIDELINES ON THE RIGHT TO PRIVACY AND THE MONITORING OF DATA

Introduction

1. These guidelines are intended to provide advice on
 - the right of staff and students to respect for their private [life and] communications
 - the circumstances in which information held in the College may be accessed, monitored or used where issues of privacy have to be taken into account.
2. Individuals need to be assured that their privacy is protected as far as is possible.
3. The College needs to ensure that it can comply with the law, uphold its own regulations and carry out its business properly.

Rights of individuals

4. The Human Rights Act 1998 came into force in 2000. This enshrines in UK law the rights and freedoms guaranteed under the European Convention on Human Rights. Article 8 is about privacy and states:
 - Everyone has the right to respect for his private and family life, his home and his correspondence.
 - There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
5. The College fully supports the principles of the Act.
6. Any interference by the College in the right to privacy will be in accordance with Article 8 and proportionate to the issue in question.
7. Any member of staff or student has the right to complain to the Principal if he or she believes their right to privacy is being interfered with unnecessarily.

Scope of information

8. The guidelines cover information that may be considered to be private as follows:
 - information that may be collected during the monitoring of operations e.g.
 - CCTV or other means of surveillance
 - data passing through the telephone or data network
 - data recorded when monitoring the College's electronic mail and web systems
 - information held by individuals at the College
 - information in paper or electronic format
 - data held on College computers
 - data held on privately-owned computers that are used for work supported by the College (where data held relating to the work of the College will, subject to Intellectual property arrangements, belong to the College)

Legislation

9. Legislation that applies in this area in addition to the Human Rights Act includes:

- Computer Misuse Act 1990
- Data Protection Act 1998
- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- and the associated Statutory Instrument, the Lawful Business Practice Regulations

Principles

10. The following principles apply in connection with monitoring of and access to data :

- The right to privacy is respected as far as is possible
- The actions taken and the use of data must be lawful
- Data must be used for the purpose for which it is collected
- The College does not routinely monitor or access any data where there may be issues of privacy but reserves the right to use or access such data under properly authorised and controlled circumstances
- Members of staff and students have a right to know the purposes for which data may be collected, accessed and used and the circumstances under which monitoring of data might take place.

Purposes/circumstances

11. The College will only permit the monitoring of or access to data as described in paragraph 8 under any of the circumstances given below.

- When the individual concerned has given permission
- When required to do so by an authorised external agency e.g. the Police
- When there is already clear evidence to indicate that the individual may be in breach of the law or College regulations and the data is critical for the progress of an associated investigation
- Where the individual is absent and access to the information is important for the work of the College

The principles described in paragraph 10 may limit the extent of the actual action taken.

Information required by external agencies

12. Only the Security Services or the Police are likely to require access to private information relating to an individual. This will usually be as part of a criminal investigation.
13. All such requests will require the appropriate warrant or documentation.
14. These requests will be handled by the Director of Human Resources in the case of staff and the Academic Registrar in the case of students. An external agency may require a single point of contact.

Information required for an internal investigation

15. There must already be clear evidence that a breach of the law or College regulations may have taken place.
16. Authorisation must be given in writing by the relevant member of the Principal's Steering Group, the Academic Registrar (in the case of students) or the Director of Information Services, who is able to provide advice.
17. The principles listed in paragraph 10 must be observed.
18. A record of the data investigation must be made and retained.

Information required for College business purposes

19. It is expected that departments and institutes will normally make prior arrangements for appropriate access to information held by an individual in order to cater for the unexpected or planned absence of the individual (including the situation where an individual has left the College). Similarly when an individual leaves the College appropriate arrangements will normally be made for access to the information held by the individual. This will cover email accounts and documents held in the office or on a computer.
20. Exceptionally and only in urgent and critical circumstances access to data held by an individual may be permitted when the information is needed for College business purposes during the absence of the individual.
21. Authorisation must be given in writing by the Head of the Department/Institute concerned.
22. The principles listed in paragraph 10 must be observed. The individual will be informed of the action being taken. Data held by the individual must not be altered.
23. A record of the data search must be made and retained and made available to the individual.

BM 8.6.05