

INFORMATION TECHNOLOGY, HIGHER EDUCATION AND THE LAW

**Matt Meyer
Eversheds
IT and E-commerce Group**

Today's Session

- Review of applicable legislation
 - Freedom of Information Act 2000
 - Data Protection Act 1998
 - Regulation of Investigatory Powers Act 2000
 - Human Rights Act 1998
- Scenarios
- Employers' liability
- Checklist of compliance



Freedom of Information Act 2000

Lord Filkin, Minister at the Department for Constitutional Affairs... “the provision of the Act will allow decisions to be effectively scrutinised, will build trust and credibility among members of the general public and also bring benefits to the public bodies themselves by acting as a drive for better records and information management in the public sector.”



Five Key Changes:

- 1) All those who contribute to decisions taken by public authorities will have to become aware of their obligations towards the Freedom of Information legislation;
- 2) Staff in public authorities will have to be trained to use clear procedures in order to respond to requests from members of the public within the 20-day timetable specified by the legislation;
- 3) Public authorities will need to get their records in order;
- 4) Each public authority will need to have a champion at board level responsible for promoting Freedom of Information;
- 5) There will have to be a real change in staff culture from a system whereby citizens are told only that which public authorities think they need to know, to one in which citizens are entitled to have access to a broad range of information.



Freedom of Information Act 2000

- comes into force 29 February 2004
- applies to public authorities, including higher education institutions
- makes information held by public authorities accessible to the public
- two complementary parts:
 - obligation to produce a publication scheme
 - responding to requests for information
- publication scheme must be approved by Information Commissioner before 31 December 2003



Freedom of Information Act 2000

- respond to requests for information within 20 working days
- some information exempt - absolute or qualified exemption (public interest test), e.g:
 - Data Protection Act subject access rights (absolute)
 - Commercial interests, trade secrets (qualified)
- enforcement is by Information Commissioner - institution can be held to be in contempt of court for refusal to comply with the Act

N.B. Codes of Practice issued by Lord Chancellor's
Department on website - www.lcd.gov.uk



EVERSHEDS

Data Protection Act 1998



Data Protection Act 1998

- processing of data must be in accordance with the data protection principles
- the data protection principles:
 - 1) fair and lawful processing
 - 2) specified and lawful purpose
 - 3) adequacy, relevance and amount of data
 - 4) accuracy
 - 5) retention and destruction
 - 6) rights of data subjects
 - 7) security
 - 8) transfers of data outside EEA



Data Protection Act 1998

- obligation to notify Information Commissioner
- different types of data, e.g. sensitive personal data has stricter requirements
- special rules apply to examination scripts and marks, confidential references etc
- enforced by Information Commissioner issuing enforcement notices
- failure to comply with a notice/processing data without notification is a criminal offence



Regulation of Investigatory Powers Act 2000

Regulation of Investigatory Powers Act 2000

- regulates interceptions/monitoring of telecommunications
- intranet, internet, fax, e-mail, telephone and voicemail
- consent generally required (sender and recipient)
- communications must be relevant to institution's business
- make reasonable efforts to inform people of interception



Regulation of Investigatory Powers Act 2000

- if no consent, interception only permissible in particular circumstances:
 - to establish the existence of facts relevant to the institution
 - to ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the institution
 - to monitor staff for quality control and staff training (but not for marketing/market research)
 - to prevent or detect crime
 - to investigate or detect unauthorised use of the institution's telecommunications systems
 - to protect against viruses



Regulation of Investigatory Powers Act 2000

- unlawful interception/monitoring/recording is a criminal offence
- remember the Data Protection Act!



Human Rights Act 1998



Human Rights Act 1998

- public authorities should comply with Human Rights principles
- relevant articles:
 - (1) Article 6 - right to a fair hearing
 - (2) Article 8 - right to respect for family and private life
 - (3) Article 10 - right to freedom of expression



Human Rights Act 1998

- Articles 8 and 10 qualified by “measures necessary in a democratic society” (e.g. prevention of crime, protection of others’ freedoms)
- proportionality
- procedures AND practice



Scenarios

Scenario 1

The Departmental Head wants the records of the internet usage of a member of a department (employee/student) for a disciplinary hearing.

Issues under Regulation of Investigatory Powers Act:

- monitoring authorised if in order to detect unauthorised use of telecommunications services.
- “unauthorised use” determined by department policy/employment contract.



Scenarios

- even if authorised, reasonable efforts to inform members of department that communications monitored.

Issues under the Human Rights Act:

- right to a fair hearing - right to respond (provide records to employee/student before hearing?)
- right to respect full private life - but qualified, e.g. by RIPA.



Scenarios

Issues under Data Protection Act:

- is the data being disclosed to a third party? i.e. is the hearing internal or external?
- other principles still apply, e.g. information must be kept securely.



Scenarios

Scenario 2

A student asks for their exam script and the breakdown of their final mark to assist in an appeal against their degree classification.

Issues under the Data Protection Act:

- exam scripts are exempt from subject access rights.
- information regarding exam marks must be supplied within 5 months of the request or 40 days after publication of the results, whichever is the sooner.



Scenarios

- cannot withhold information regarding exam marks due to unpaid fees, unreturned equipment etc
- information must be provided without amendment or deletion.

Issues under the Freedom of Information Act:

- student has subject access rights to information about marks under DPA/FOIA not applicable.
- could student ask for script as FOIA request?



Scenarios

- public interest test - not likely to be satisfied.

Issues under the Human Rights Act:

- right to a fair hearing? Should provide all relevant evidence - but query whether applicable to internal appeals.



Scenarios

Scenario 3

The institution has taken legal advice regarding a controversial planning application. That advice has the benefit of legal professional privilege. A member of the public asks what advice has been given to the institution.

Issues under the Freedom of Information Act:

- advice will not have been included in the publications scheme (!)



Scenarios

- legally privileged information is exempt BUT
- the exemption is not absolute - is it in the public interest to disclose it or withhold it?!
- not in public interest that legal advice loses confidentiality but public has an interest in outcome of planning decisions.
- N.B. institution can withhold information if it has already decided to publish it at some future date.



Scenarios

Scenario 4

You receive a telephone call from a parent in the USA asking whether their son has regularly attended lectures over the previous year.

Issues under the Data Protection Act:

- fair and lawful processing - has student given consent?
- other justification - legal obligation, performance of a contract?
- accuracy - could another student forge attendance records?
- for how long should records be kept?



Scenarios

- transfer of data outside the EEA.
- if request made by police, would be in standard written form.

Issues under Freedom of Information Act:

- absolute exemption - would breach student's data protection rights.



Scenarios

Scenario 5

A student's e-mails and internet usage have been intercepted and it is discovered that she has links to a suspected terrorist organisation.

Issues under the Regulation of Investigatory Powers Act:

- should it have been intercepted? Allowable if to prevent/detect crime/unauthorised use
- must still have made efforts to inform student re interception



Scenarios

Issues under the Data Protection Act:

- sensitive personal data (political opinions/commission or alleged commission of an offence)
- special circumstances apply to processing sensitive personal data where no consent given - include administration of justice
- other principles will still apply (e.g. information must be kept secure, not retained for longer than necessary etc.)



Scenarios

Issues under the Human Rights Act:

- right to freedom of expression and to receive and impart ideas without interference
- qualified by protection of rights/freedoms of others
- balancing act - political opinion, or danger to society?



Scenarios

Scenario 6

An employee requests information held by his employer regarding his prospects of promotion.

Issues under the Data Protection Act:

- employee has subject access rights - but exempt to the extent that negotiations regarding promotion would be prejudiced.
- if information is provided, must not be amended beforehand.



Scenarios

Issues under Freedom of Information Act:

- if employee does not have data protection subject access rights then there is a qualified exemption under the FOIA.
- Is it in the public interest?

Issues under Regulation of Investigatory Powers Act:

- do performance reviews include information about employee's communications?
- allowable if e.g. to ascertain compliance with regulatory procedures, to monitor staff, etc.



Scenarios

- does institution's policy include what communications will be monitored and how they are relevant to performance reviews?

Issues under the Human Rights Act:

- right to a fair hearing - again, provide as much evidence as possible (but unlikely to apply to negotiations regarding promotion).
- right to respect for private life, including correspondence - to what extent is the information in the reviews relevant to promotion prospects?



Employers' Liability

- In general, an employer can be held liable if an employee breaches a legal obligation
- Freedom of Information Act
 - persistent failure to comply will mean institution is in contempt of court
 - does not give rise to any right to bring civil proceedings against authority



Employers' Liability

- Data Protection Act
 - the institution will be held liable for a breach BUT
 - directors/managers who are responsible (even if only through neglect) can be found guilty of an offence
- Regulation of Investigatory Powers Act
 - again, both the institution as a whole and a director/manager responsible can be found guilty of an offence



Employers' Liability

- Human Rights Act
 - if an employee of a public authority breaches the Act, the public authority will be held liable if the victim of the breach brings proceedings against it



Checklist for Compliance

- start work on a publication scheme
- check out the Codes of Practice - www.lcd.gov.uk and the higher education model action plan at www.jisc.ac.uk
- clarify your institution's policies on the retention, management and retrieval of data
- notify the Information Commissioner if you have not already done so
- train staff in responding to requests for information under FOIA and DPA



Checklist for Compliance

- make sure employees and students know when their communications may be intercepted, monitored or recorded
- only intercept communications if you have a good reason
- keep an eye out for human rights!



INFORMATION TECHNOLOGY, HIGHER EDUCATION AND THE LAW

MATT MEYER

mattmeyer@eversheds.com



EVERSHEDS