Data Protection
In and Out of the Cloud

SFCF IS Conference
Birmingham, 17 May 2012
Hi!

• Jason Miles-Campbell
  JISC Legal Service Manager

• jason.miles-campbell@jisclegal.ac.uk

• 0141 548 4939

• www.jisclegal.ac.uk
Legal Guidance for ICT Use in Education, Research and External Engagement

- Copyright & IP
- Data Protection
- Freedom of Information
- Human Rights
- e-Commerce
- Accessibility Law
- Defamation
- Harassment
- Terrorism
- Interception and Monitoring
- Hostile Liability
- Employment Law
- Health and Safety

**News**

JISC Podcast on the JISC Legal's Kirsty McInnes about what the Digital Universities and Colleges Agreement means.
(Posted on 24/07/2010)

Umbrella Data Protection: The European Commission’s recent amendment of the Data Protection Directive means that a data protection agreement must be put in place for data transfers outside the EU for a data protection agreement provision.
(Posted on 23/07/2010)

Government Committed to New Libel Bill
Defamation Bill, to be published next year, will balance freedom of speech with protection of reputation.
(Posted on 19/07/2010)

Facebook's Privacy Under German Investigation
DP Officer claims Facebook's collection and retention of non members' private data breaches privacy laws.
(Posted on 12/07/2010)

**Events**

JISC Legal at JISC Innovation Forum 2010 (28/07/2010)
JISC Legal will be participating in a panel discussion on Intellectual Property Rights and Licensing: Current Approaches and Future Impact at the JISC Innovation Forum 2010 at the Royal Holloway, University of London.

On 23 July 2010, JISC Legal's Jason Miles-Campbell will be presenting at the UKOER10 International Showcase, on the legal issues associated with Open Educational Resources and intellectual property.

**Guidance**

e-Safety Background Video for England
Background Video for England
Safeguarding: Meeting your e-safety duties
(England)
Law, ICT and Sixth Form Colleges

Please Note: This guidance is for information only and is not intended to replace legal advice when faced with a risk decision.

Table of Contents
1. What's in this Guidance?
My knowledge of DP law is...

1. It’s my Mastermind specialist subject
2. I deal with DP issues on a weekly basis
3. I’m clear on the basics, nothing too tricky
4. A brief acquaintance, but ask others
5. What does DP stand for, then?
6. I’m not at liberty to tell you for DP reasons
• Data Protection Act 1998
• Information Commissioner
• Other relevant law:
  Freedom of Information Act 2000
  Privacy and Electronic Communications Regs 2003
  Protection of Freedoms Act 2012
Why Comply?

- It’s the law
- Good business practice
- Sets a good example
- Confidence
- Identity theft – the risks
Some DP Terminology

• Data Subject
• Data Controller
• Data Processor
• A Relevant Filing System
• Processing
What is Personal Data?

• Any information which relates to an identified or identifiable person

• Living persons

• Must be significant biographical information which affects privacy

• Sensitive personal data
Notification

• Notification Info Commissioner before processing
• Notification includes statement of purposes
• Check to ensure your processing is covered
• Processing without notification is illegal (unless exempt)
Common Scenarios

- Police request information on one of your students
- A parent requests information on son’s attendance
- Internal sharing of data amongst staff
- Using external computing services (e.g. “Cloud”)
- External sharing of data
  - All have DP compliance implications
Data Protection Essentials

“Data protection ..regimes...do not seek to protect data itself, rather they seek to provide the individual with a degree of control over the use of their personal data”

“data privacy regimes do not seek to cut off the flow of data, merely to see that it is collected and used in a responsible and, above all, accountable, fashion” (Source: DP Code of Practice for FE and HE)

i.e. Data Protection law does not prevent using and sharing personal data but .. Criminal Justice and Immigration Act 2008 – gives ICO power to impose fines direct for serious security breaches
The Data Protection Principles

Data Protection Act 1998

Schedule 1
Principle 1 – fair and lawful processing

To process, a Schedule 2 condition must be met:

• Consent
• Legitimate interest of the data controller
• Fulfilment of a contractual obligation
Principle 1 – fair and lawful processing

To process sensitive data (Schedule 3):

• Explicit consent
• Fulfilment of employment law
• Protection of vital interests
• Needed for administration of justice / legal proceedings
Principle 2 – limited purposes

• Consider all uses and future uses

• State the purposes when collecting the data

• Stick to using the data for those purposes

• If a further purpose arises, you need to seek further consent
A Sample

Data Protection Statement

JISC Legal undertake to treat your personal data in accordance with the provisions of the Data Protection Act 1998. The data given will only be used to register you for the JISC Legal Newsletter on the JISCmail system. You can read the details of our Privacy policy at www.jisclegal.ac.uk/privacystate.htm
Principle 3 – adequate, relevant, not excessive

• Follows from purposes
• Good records management practice
• See JISC infoNet
• No duties with respect to personal data you no longer hold!
Principles 4 & 5 – Accuracy and Currency

• Principle 4 –
  Data must be accurate and kept up-to-date

• Principle 5 –
  Data must be kept no longer than necessary
Principle 6 – the individual’s rights

• S.7 the Data Subject Access request
• Allows access to personal data
• Exemptions:
  – request not in writing, or fee not paid; requester cannot verify identity; disclosure of third party personal data; disclosure of third party as source; certain health, education social work records
Principle 6 – the individual’s rights

• S.10 Substantial prejudice

• S.12 Right to stop automatic processing
Principles 7 – Security

Principle 7 –

Data must be secure

(organisationally and technically)
Information Security

Criminal Justice and Immigration Act 2008 – gives ICO power to impose fines direct for serious security breaches. Check:

• Password and access, encryption for mobile technologies
• Authority to transfer/share information with third parties – see section in Code of Practice
• Compliance with recognised standards – what the ICO expects?
• UCISA Information Security Toolkit may help
1. Very secure
2. Secure
3. Neutral
4. Not secure
5. Dicing with disaster
6. It depends on who the provider is and what you’ve signed up to, funnily enough
Principle 7 - security

Organisational

– Systems
– Procedures
– Personnel
– Physical access
Principle 7 - security

Technical

- Hacking
- Logging
- Tracking
- Transfer
Principle 8

• Principle 8 – Data must not be sent out of Europe without suncream
1. We adopted, reassured as to DP
2. We adopted without reassurance about DP
3. We considered and rejected cloud because of DP
4. We considered and rejected cloud for other reasons
5. Haven’t considered/don’t know
1. We know data held in Europe
2. Data held elsewhere, but measures in place (e.g. *safe harbor*)
3. We hope Amazon/Microsoft/Google have sorted this out...
4. Haven’t given it much thought
5. Not applicable
Important DP points

When collecting personal information, consider:

1. **Purpose**: why are you collecting personal data,

2. **Fairness**: is the reason fair to the data subject and

3. **Transparency**: does the data subject know about it

4. **Security**: at an appropriate level of security
What every Sixth Form College should have

• DP policy in place and a regular review date

  New developments which may affect your DP policy:

• Mechanism for conducting a privacy impact assessment at planning stage of new project

• Guidance for staff student use of social networking and web 2.0 tools

• Guidance for staff on laptops memory sticks and other ‘mobile’

• Information Security standards

• Website information on privacy and cookies
Website

Should have a privacy statement which
• Complements full DP policy
• States what is done with information collected
• Cookie regulations – here comes 26 May 2012
Scenarios

• Police request personal information on one of your students
• A parent requests information on attendance of student
• Internal sharing of data amongst staff
• External sharing of data
Police request personal information on one of your students

1. No problem!
2. Mmm... need more info
3. Not a chance.
4. I can see me being dragged off in handcuffs any second
5. Haven’t a clue
A parent requests information on student’s performance

1. No problem!
2. Mmm... need more info
3. Not a chance.
4. I can see me being dragged off in handcuffs any second
5. Haven’t a clue
• DP Code of Practice
• JISC Legal – sector specific guidance
• College stuff e.g. AoC
• UCISA Information Security Toolkit and others
  http://www.ucisa.ac.uk/publications.asp
• ICO – privacy impact assessments / general guidance
• JISC InfoNet on records management and data retention
Summary

• Ensure awareness of data protection
• Periodically review what personal data you hold
• Ensure your notification allows this
• Ensure you’ve stated the purposes for which the data will be used
• Ensure that the data protection principles are being observed
Any Questions?

www.jisclegal.ac.uk
info@jisclegal.ac.uk
0141 548 4939
1. Excellent
2. Good
3. Of little value
4. Bad
5. Worse thing I’ve sat through since I was made to watch Britain’s Got Talent
6. Would prefer not to hurt presenter’s feelings / undecided