



KING'S
College
LONDON

University of London

Policies, practices and the law: information compliance at King's

Jan Booth – Head of Information Governance and
Compliance

Structure

- **Framework** – policies that define information compliance and organisation of the compliance function
- **Support** – practical support for policy implementation
- **Monitoring and interception** – interaction between the law, local procedures and technology
- **Access and disclosure** – valuable College services, but not without implications
- **Conclusion** – so, why did we get involved in this?

Framework

College Regulations

- Core policy document binding on all staff and students
- Includes the Information Services and Systems (ISS) Regulations
- Reviewed annually, approved by the College Council and Academic Board

Specific policies

- Information Security Policy – follows the principles of ISO 27002
- E-communications Policy – incorporates the JANET AUP
- IT Monitoring Policy – draws on the JISC model policy
- Data Protection Policy – a new British Standard is due next year
- Policies set the context, they don't define the detail

Bringing the function together

- Implementation requires a multi-disciplinary approach
- IT professionals, compliance and information management specialists
- Groups and meetings include – IT Security Group, ISS Legal Compliance and Information Governance Committee, College Audit and Compliance Committee

Support

IT security

- Published documentation setting out practices and procedures
- Online guidance and tools
- Bespoke arrangements for research projects as required

Information management approach

- Still developing in the context of IT infrastructure renewal
- New work on identifying and classifying data
- Records management toolkit
- Compliance training
- Compliance audits

Data retention

- Long standing implementation of the sectoral records retention guide
- Lack of granularity and problems of interpretation
- Project to update, revise and mandate

Monitoring and interception

- Routine monitoring activities are set out in the IT Monitoring Policy
- Includes monitoring individual users and intercepting email
- Legally – interplay between the Regulation of Investigatory Powers Act (and the associated Telecommunications Regulations), the Human Rights Act and the Data Protection Act
- Procedurally – close working between ITS and the Legal Compliance team
- Email interception is rare
- For certain types of infringing content the implications are severe, see the Terrorism Act 2006 for instance

Access and disclosure

- Centralised logging and clearance of access requests under the Data Protection Act (DPA) and Freedom of Information Act (FoIA)
- DPA typically sees enquiries from staff and students; occasionally external, for instance from the Police
- FoIA enquiries are often from journalists, businesses or special interest groups
- Enquiries can be complex and often political; can sometimes involve walking a tightrope!

Why did we get involved in this?

- A challenge for integrated information departments
- Technical infrastructure v information infrastructure; enablers or killjoys?
- We're still finding the balance at King's but we're working together constructively and we're delivering significant value to the College

Jan.booth@kcl.ac.uk