

# Identifying Data Protection Issues

Developing Lifelong Learner Record Systems and ePortfolios in FE and HE: Planning for, and Coping with, Legal Issues.

# Knowing what we know...

- Development of LLR/ePortfolio systems will inevitably increase personal data holdings and electronic transfers between institutions
- DP law will require institutions to meet certain standards with regard to that processing.
- Institutions (and groups of institutions) need to understand the:
  - purposes, nature and scope of their processing
  - flows of data within the LLR/ePortfolio system
  - appropriate administrative & technical responsibilities
  - legal relationships arising from those responsibilities.

# The Data Protection Principles

- Personal data shall be:
  - processed fairly and lawfully & only if certain conditions are met (Schedules 2 & 3 DPA);
  - obtained only for specified & lawful purposes;
  - adequate, relevant and not excessive.
  - accurate and, where necessary, kept up to date.
  - kept for no longer than is necessary.
  - processed in accordance with data subjects' rights.
  - protected against unauthorised or unlawful processing & accidental loss, destruction, or damage.
  - only transferred to non-EEA countries ensuring an adequate level of protection.

# Planning Compliance

- Build compliance into the planning/design process.
  - Proposed uses of personal data
  - 3<sup>rd</sup> parties from whom data may be received
  - 3<sup>rd</sup> parties to whom data may be transferred
  - Risks identified & institutional responses documented.
- Institutional data protection officers should always be involved in this process – notification.
- Later changes to the system, technical & administrative, should also be reviewed and DP implications documented before implementation

# Mapping a System - UEO I

- Identifying the data protection actors
- Identifying proposed purposes for data transfers and processing
- Determining data protection roles
- Considering categories of personal data to be processed/transferred
- Identifying personal data that is 'sensitive personal data'

# Mapping a System - UEO II

- Determining which processing conditions might justify the processing/transfer
- Choosing processing conditions
- Dealing data subject consent
- Determining when collection notices should be provided to data subjects
- Dealing with data subject access

# Mapping a System - UEO III

- Plotting necessary contractual agreements between data protection actors
- Considering necessary administrative documentation
- Plotting the necessary institutional infrastructures
- Identifying probable information dissemination and training needs

# Lessons from the UEO Example

- Most FE/HE institutions will be largely compliant with DP obligations as regards internal learner records/ePortfolio systems
- Problems are likely to arise where PD is transferred between institutions, if data controller staff are not clear what conditions attach to its processing
- One key element of the mapping process is to identify responsibility and liability – see also the NIIMLE project.
- The other key element is ensuring that the rights of data subjects are adequately protected – a system that data subjects don't trust to protect their personal data is unlikely to be used effectively.

# Processes and Practices

- Creating processes for DP compliance is relatively straightforward
- Ensuring that staff practice conforms with those processes is perhaps more difficult
- Proper process utilisation may require other institutional changes – employment contract clauses, information audit, compulsory training
- Both processes and practice will require re-evaluation on a regular basis, as technologies and data subject expectations evolve.