

# **Assessment of the ISEB Certificate in Data Protection**

The British Computer Society (BCS) describes the ISEB Certificate in Data Protection as providing “an entry point qualification for those with data protection responsibilities, as well as providing an effective conversion route for those needing to update their knowledge of and practice under the 1984 Data Protection Act.”

They go on to say that, “On completion candidates should be able to:

- Understand the broader context of the Act, its origins and the reasons for data protection legislation;
- Outline a detailed understanding of how to apply the data protection principles and the standards the Act promotes to given sets of circumstances;
- Understand the way in which the Data Protection Act works;
- Gain a broad understanding of what has to be done to achieve compliance.”

### **Providers**

The course assessed was run by QT & C Limited, however, it was not assessed with a view to recommending a particular course provider and the qualification can be undertaken with several companies (information from BCS website):

#### **British Standards Institution**

389 Chiswick High Road, London, W4 4AL

Tel: + 44 (0)208 996 7180 Fax: + 44 (0)208 996 7448

Email: [cservices@bsi-global.com](mailto:cservices@bsi-global.com)

Website: [British Standards Institution](http://BritishStandardsInstitution.com)

Format: 8 x 3 hour training modules (four per week over two days for two consecutive weeks).

#### **Morgan Cole Solicitors**

Apex Plaza, Reading, RG6 4NZ

Tel: +44 (0)118 955 3000 Fax: +44 (0)118 939 3210

Email: [iseb@morgan-cole.com](mailto:iseb@morgan-cole.com)

Website: [Morgan Cole Solicitors](http://MorganColeSolicitors.com)

Format: five-day course

#### **Pinsent Masons - International Law Firm**

Legal Training Services

30 Aylesbury Street, London, EC1R 0ER

Tel: + 44 (0)20 7490 6218 Fax: + 44 (0)20 7490 2545

Email: [Pinsent Masons](mailto:PinsentMasons.com)

Website: [www.pinsentmasons.com](http://www.pinsentmasons.com)

Contact: Helen Hadjipantelis

Format: 5 days

Limited free places for candidates from voluntary or charity sectors.

#### **QT&C Limited**

Cranfield Innovation Centre, University Way, Cranfield Technology Park, Cranfield, Beds, MK43 0BT

Tel: + 44 (0)1234 436085 Fax: + 44 (0)1234 752514

Email: [contact@qtandc.co.uk](mailto:contact@qtandc.co.uk)

Website: [QT&C Ltd](http://QT&CLtd.com)

Contact: Nathan Fowler

Format: 5 day course

Concessions available for the public sector.

## Aim

The course was undertaken to assess whether an ISEB certificate in Data Protection would meet the data protection training requirements of Caldicott Guardians and others with Data Protection responsibilities, e.g. IG Managers, DP Officers and DP support staff.

The course was assessed regarding whether it:

1. Is appropriate to health and social care settings
2. Covers the requirements placed on organisations by the Caldicott Principles
3. Will assist organisations to comply with any requirements within the IG Toolkit

## Syllabus

The syllabus is set by ISEB and all providers must deliver a course that covers at least 80% of the following:

- **Context** - this concentrates less on the early history of data protection in the 1970's and more on the relationship with privacy and human rights and the key events since 1980 in the development of the legislation.
- **Law - Data Protection Act** - covering the main concepts of the 1998 Act and subordinate legislation.
- **Law - Telecommunications Regulations** - covering the relationship of the regulations to the Data Protection Act.
- **Law - Associated Legislation** - to include relevant parts of legislation such as Freedom of Information Act, Regulation of Investigatory Powers Act, etc., which impact upon the Data Protection Act.
- **Application** - how compliance is achieved and the Act works in practice.

# Assessment

## 1. Is the ISEB Certificate in Data Protection appropriate for staff working in health and social care settings?

The assessed course was structured as below, and on each day the content was made relevant to the work environments of the delegates

### Day One

- Discussion of the various data protection legislation within the British Isles
- The concept of privacy
- Setting data protection within a historical perspective – discussion of the ‘data protection timeline’, i.e. progress within data protection from 1948 to 1998
- The main changes from the Data Protection Act 1984
- The relationship between privacy and the Data Protection Act 1998
- Data Protection Act 1998 Key definitions – data; personal data; processing; relevant filing system; accessible records (health, education, social services)

### Day Two

Revision of Day One topics

- Data Protection Act 1998 More key definitions – data subject; data controller; data processor; recipient; third party; sensitive personal data;
- Processing for the Special Purposes (journalistic, literary and artistic purposes)
- The Data Protection Principles – overview of the eight principles
- Principle 1 – fair and lawful processing in accordance with Schedule 2 and 3 conditions.

### Day Three

Revision of Day Two topics

- Principles 2 – 8
- Confidentiality and breach of confidence
- The Caldicott Principles
- Principle 6 – the rights of the individual, i.e. subject access, prevention of damage/distress and direct marketing; automated processing; rectification etc; compensation; requests for assessment of processing

- Principle 7 –appropriate organisational and technical security measures.  
Discussion of the BS / ISO 27000 series (commonly known as ISO 17799 / BS 7799)

#### **Day Four**

Revision of Day Three topics

- Principle 8 – overseas transfers of personal data
- The role of the Information Commissioner
- The Information Tribunal
- Notification
- Exemptions from the Data Protection Act

#### **Day Five**

Revision of Day Four topics

- Data Protection Act Offences
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Preference Services – the services that enable opt out from direct marketing
- Associated legislation – e.g. the Computer Misuse Act 1990; the FOI Act 2000; the Regulation of Investigatory Powers Act 2000 and Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000

## **2. Does the ISEB Certificate in Data Protection cover the requirements placed on organisations by the Caldicott Principles?**

The Caldicott Committee found that the patient information flows within the NHS were necessary for the effective working of the NHS; however, they identified several weaknesses in the way that patient identifiable information was transferred. They developed six principles for the safe and secure handling of patient identifiable information:

### **F - Formal justification of the purpose**

*Look at the reasons behind the flow of the information, who is the sender, where is it sent to, and what does the recipient do with it?*

The purpose of processing personal data was well covered on the assessed course, in particular in being able to inform the data subject why the information is required, what use will be made of it and whether it will be shared.

### **I - Information transferred only when necessary**

*Is the transfer necessary and, if it is, can the information be transferred more securely?*

Transfer of personal data was discussed at length in relation to necessity, e.g. could another method be used, and also in relation to ensuring information is kept secure during transfer. Overseas transfer of information was also covered in depth.

### **O - Only the minimum patient-identifiable information**

*Will the NHS number or a local identifier suffice rather than using name, address etc.*

Practical examples were utilised to assist delegates to make decisions on whether personal information was required, and if so whether all the information requested was actually needed.

### **N - Need to know access controls**

*Consider who needs to have access and where possible build in access controls so that each member of staff has access only to information they need to carry out their role.*

Access to information was discussed in relation to ensuring personal information remained confidential, security measures that could be put in place and penalties for breach of confidentiality or of the security measures.

### **A - All understand their responsibilities**

*Use induction and mandatory training to ensure all members of staff are informed of and kept updated about their legal, organisational and professional responsibilities.*

The course not only covered the Data Protection Act in depth, but also related legislation with a discussion of local and professional policies and obligations that individuals must comply with.

### **C - Compliance with the law**

*Appoint a senior manager to lead on compliance issues, so that common law duties and legislative provisions are not breached.*

Penalties for breaches of confidentiality and for breaches of the Act were well covered. There was also detailed discussion about criminal offences under the Data Protection Act, with practical and relevant examples.

### **3. Will the ISEB Certificate in Data Protection assist organisations to comply with any requirements within the IG Toolkit?**

The assessed course material addressed several areas of the IG Toolkit. In particular, elements of:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance

#### **Information Governance Management**

The ISEB Certificate in Data Protection is obviously relevant to the training, awareness and staff responsibility requirements within the IG Toolkit. The specific requirements addressed are:

- 102 The Trust's ability to access expertise across the Confidentiality and Data Protection assurance agenda
- 112 Staff induction procedures that effectively raise awareness of Information Governance
- 113 The assessment of staff training needs and provision of job/role specific information governance training

#### **Requirement 102**

An ISEB in data protection is appropriate for those involved in the Caldicott function and the Confidentiality and Data Protection work programme. Depending on organisational structures, the qualification could be appropriate for Caldicott Guardians, Information Governance Managers, Data Protection leads and Data Protection support staff. Aspects of the course will also be of value to those staff directly involved in responding to subject access requests and those responsible for communications about the processing of personal data.

#### **Requirement 112**

The depth of the information provided on the assessed course would be unnecessary for induction purposes. However, it would be appropriate for the member of staff responsible for providing confidentiality and data protection induction to undertake an ISEB in Data Protection. The knowledge gained on the course could then be tailored to specific audiences.

#### **Requirement 113**

Where training needs analyses for staff directly involved in the Caldicott function and the Confidentiality and Data Protection work programme reveal a need for in depth training, the ISEB is an appropriate qualification. As with Requirement 112, cascade training could then be provided for other staff processing personal information.

#### **Confidentiality and Data Protection Assurance**

As expected many of the requirements within this initiative are addressed on the assessed course, in particular:

- 201 Confidentiality code of conduct
- 203 Informing patients about proposed uses of their information
- 204 Enabling patients to ask detailed questions about processing of their data
- 205 Recognising and responding to subject access requests
- 208 Safe haven procedures

- 209 Transfers of personal data to countries outside the European Economic Area

#### **Requirement 201**

The course covers personal responsibilities for ensuring that the processing of personal data is within the law and the penalties for failure to do so. There was discussion about the professional codes of confidentiality that might apply, including the NHS Code.

#### **Requirement 203 and 204**

The assessed course provides in depth information on fair collection/processing notices required under the DPA. This included details on what data subjects must be fully informed of and the circumstances in which information may not have to be given.

#### **Requirement 205**

Recognising and responding to requests for information (subject access requests) is very well covered in the course.

#### **Requirement 208**

The assessed course covers the Caldicott Principles and the security measures necessary to keep personal information safe at all stages were discussed in depth

#### **Requirement 209**

This was well-covered, with discussion of several scenarios of organisations located within and outside of the European Economic Area

### **Information Security Assurance**

Appropriate security measures when processing personal data were covered during discussions about Principles 7 and 8 of the Act. However, there is an ISEB in Information Security for staff requiring more in depth training. Specific requirements touched on were:

- 306 Access rights to personal data
- 307 Information assets
- 308 Sharing information with other organisations
- 309 Ensuring the availability of information processing facilities, etc

#### **Requirement 306**

This was covered in relation to actually having access controls in place to secure personal information and also as regards monitoring staff use of organisational systems.

#### **Requirement 307**

Information asset registers were discussed with particular emphasis on the inclusion of all assets, i.e. information, software, people, physical and services. The importance of creating a single corporate asset register was also covered.

#### **Requirement 308**

The security measures necessary to keep personal information safe at all stages were discussed in depth. Monitoring of employees was also covered in relation to the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

**Requirement 309**

The course contains information about risk assessments, the creation of back-ups and the need for business continuity plans.

**Conclusion**

The Data Protection Act 1998 applies to all health and social care organisations, and also to individuals carrying out work for those organisations. The ISEB Certificate in Data Protection is therefore highly relevant to all working in the data protection and confidentiality fields in health and social care settings.

The assessor has worked in the confidentiality and data protection field for several years and found the course method of relating legislation to practical applications in diverse work places to be of great value. Caldicott Guardians and IG Managers should find an ISEB Certificate in Data Protection a valuable addition to their understanding and knowledge of data protection and confidentiality. The course is almost a prerequisite for all those responsible for data protection in an organisation.

The requirements within the Caldicott Principles were addressed throughout the course as they directly relate to the obligations under the Data Protection Act 1998. Providers offering onsite courses are able to tailor the content to make it more NHS specific, with the possibility of covering the Caldicott Principles as a separate topic.

The knowledge gained from the range of material covered in the course would assist IG staff in meeting requirements in several initiatives within the IG Toolkit.