

# **ISEB Certificate in Data Protection Syllabus**

**Version 6.1**

**May 2011**

# Contents

---

Change History .....	2
Rationale/Background.....	3
Aims and Objectives .....	3
Target Group .....	3
Pre-Requisite Entry Criteria for the Course.....	3
Format of the Examination.....	4
Pass Mark.....	4
Syllabus Content and Learning Objectives .....	5
1. Context (2.5% - 1 hour of course work) .....	5
2. The Law (52.5% - 21 hours of course work) .....	5
3. Application (45% - 18 hours of course work) .....	8
Additional Information .....	10
Levels of Skill and Responsibility (SFIA Levels) .....	10
Level 1: Follow.....	10
Level 2: Assist.....	10
Level 3: Apply .....	10
Level 4: Enable .....	10
Level 5: Ensure and advise.....	11
Level 6: Initiate and influence .....	11
Level 7: Set strategy, inspire and mobilise.....	11
Levels of Knowledge (K Levels).....	12
Level 1: Remember (K1).....	12
Level 2: Understand (K2) .....	12
Level 3: Apply (K3) .....	12
Level 4: Analyse (K4).....	12
Level 5: Synthesise (K5).....	12
Level 6: Evaluate (K6) .....	12
Examination Details .....	13
Trainer Qualification Criteria .....	13
Classroom Size.....	13

## Change History

<b>Version Number</b>	<b>Changes Made</b>
V6.1 May 2011	<p>Additions:  Warrants (entry/inspection) (2.1.2.1)  ICO new enforcement powers (2.1.2.1) including s55 (3A)</p>
V6.0 April 2011	<p>Syllabus V5.7 recast using new standard syllabus template and with minor amendment of language. Also revised in light of recent changes in DP law.</p> <p><b>Additions:</b>  ICO new enforcement powers (2.1.2.1)  Undertakings (2.1.2.1)  CoP on data-sharing (s52A-E) (2.1.2.3)  Two-tier notification fee regime (2.1.3)  Legal professional privilege (2.1.6)  Subject information provisions (2.1.6)  Non-disclosure provisions(2.1.6)</p> <p><b>Deletions:</b>  Assessable processing (old Part 2A,C3)  Traffic/billing data; cli; directories (old Part 2B, A2, A3 &amp; A4)  Defamation Act 1996 (old Part 2C, A6)  Enforced subject access (old G3, Part 3)</p> <p><b>Clarifications/qualifications:</b>  s29 (2.1.6)  s32 (2.1.6)  Subject access fees (2.1.5)  ICO CoPs (2.1.2.3)  Law of confidence (2.1.4)</p> <p><b>Amendments:</b>  See 3.1 including introduction of Privacy by Design and PIAs.  See 3.3 - NB access controls, encryption covered by topic of complying with 7<sup>th</sup> principle in 3.1</p>
5.7 Oct 2009	Formatted. Added a change history to the document and added the new logo.
5.6 May 2008	Updated the syllabus so that Context is now examinable and included the Criminal Justice and Immigration Act.
5.5 Nov 2007	Transitional Provisions was removed from the syllabus and Research Exemption has been added as a specific exemption.

## **Rationale/Background**

Organisations need to be aware of their obligations under UK data protection law, in particular the Data Protection Act 1998 (“the Act”). The ISEB Certificate in Data Protection is designed for those with some data protection responsibilities in an organisation or who, for other reasons, wish to achieve and demonstrate a broad understanding of the law and its practical application. It is recognised that those with overall responsibility for data protection within an organisation will need to develop a more detailed understanding of the law, including those provisions which are not covered in the syllabus.

## **Aims and Objectives**

Thinking from a candidate’s point of view, what is the qualification designed to achieve and how will it contribute to them professionally?

The Certificate in Data Protection is intended to promote an understanding of the practical application of UK Data Protection law including placing it in a human rights context. By obtaining the certificate individuals will possess:

- A recognised qualification in data protection.
- An understanding of the way that the Act and the Privacy and Electronic Communications (EC Directive) Regulations 2003 work.
- An understanding of what has to be done to achieve compliance.
- A broad appreciation of the wider context of the Act.

## **Target Group**

The qualification is aimed at those who have, or wish to have, some responsibility for data protection within an organisation. However, it will also be useful for others who wish to obtain, and demonstrate, a broad understanding of the UK’s data protection regime.

## **Pre-Requisite Entry Criteria for the Course**

There are no mandatory requirements for candidates though candidates will need a reasonable standard of written English. However, this is quite a demanding course. Those candidates who already have some grasp of data protection law, particularly experience of applying it in a work context, will be at an advantage. Other candidates are likely to find the course daunting unless they have had some legal training, or experience of, or an aptitude for, applying the law.

**Format of the Examination**

The examination is a three hour closed-book examination comprising three sections. The format is as follows with a balance of questions across the syllabus.

**Section A**

20 multiple choice questions (1 mark each). All questions to be attempted.

**Section B**

8 short answer bullet point questions (5 marks each). All questions to be attempted.

**Section C**

6 essay style questions (10 marks each). 4 questions to be attempted. Longer more detailed responses are required. Whilst some questions will require a detailed explanation of provisions of the law, others will require discursive answers covering the practical application of the law in particular circumstances.

**Pass Mark**

The pass mark is 50 out of 100 (50%).

Distinctions will be awarded to candidates who achieve 80 or more (80%).

## **Syllabus Content and Learning Objectives**

### **1. Context (2.5% - 1 hour of course work)**

The objective is to ensure a basic appreciation of the context of data protection law and in particular that privacy is wider than data protection.

#### **1.1 What is privacy? K2**

1.1.1 The right to private and family life and the relevance of confidentiality.

1.1.1 European Convention on Human Rights and Fundamental Freedoms, UK Human Rights Act

#### **1.2 History of data protection legislation in the UK**

1.2.1 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980

1.2.2 Council of Europe Convention 108, 1981

1.2.3 Data Protection Act 1984

1.2.4 Data Protection Directive 95/46/EC

1.2.5 Telecommunications Directive 97/66/EC, Privacy and Electronic Communications Directive 2002/58/EC, and subsequent revisions of the latter.

**NB Candidates are not expected to have a detailed knowledge of the above.**

### **2. The Law (52.5% - 21 hours of course work)**

As this is a certificate course and only 21 hours are allocated for instruction on this part of the syllabus, knowledge and understanding of the whole Act is not expected.

#### **2.1 Data Protection Act (45% 18 hours course work)**

##### **2.1.1 The definitions**

The objective is to ensure that candidates know, and understand the major definitions in the Act and how to apply them in order to identify what information and processing activities are subject to the Act.

- Data (including relevant filing system, accessible records and category (e) unstructured data)
- Personal data
- Processing
- Data Subject
- Data controller
- Data Processor
- Recipient
- Third Party
- Sensitive Personal Data
- The Special Purposes

Though candidates are expected to be aware that the Freedom of Information Act (FOI) 2000 created a new category of data, category (e) data, they are not expected to understand the implications of this in respect of the section 7 right of subject access and are not expected to cover s33A(1) and s33A (2).

Candidates should have a broad understanding of the reason for making provision in respect of the special purposes, namely to seek to strike an appropriate balance between freedom of expression and privacy. They will not be expected to have a detailed understanding of sections 32 (see 2.1.6), or 44. They are not expected to be aware of sections 45 and 46

### **2.1.2 The Role of the Commissioner K2**

The objective is to ensure an understanding of the role and main powers of the Information Commissioner. The following are to be covered.

#### **2.1.2.1 Enforcement** (including roles of the First-tier Tribunal and the Courts)

- Information and Enforcement Notices
- Prosecution
- Warrants (entry/inspection) (Schedule 9,1(1) & 12 only – that is a basic understanding of grounds for issuing and nature of offences)
- Assessment Notices (s41A-s41C) including effect of s55 (3) added by Coroners and Justice Act 2009 which provides that the Information Commissioner may not issue a monetary penalty notice in respect of anything found in pursuance of an assessment notice or an assessment under s51(7).
- Monetary penalties (s55A-55E) including the effect of the s55 (3A) provision.
- Undertakings (NB candidates are required to have a basic understanding of how the ICO uses ‘undertakings’ and that they do not derive from any provision in the DPA98. They are not expected to know the detail of their status and provenance).

#### **2.1.2.2 Carrying out s42 assessments**

**2.1.2.3 Codes of Practice** (including s52A-52E Code of Practice on data sharing) and all current ICO issued Codes.

### **2.1.3 Notification**

The objective is to ensure a broad, but not detailed, understanding of the notification scheme and a grasp of how to apply the notification exemptions.

- Information to be notified and the public register.
- The exemptions from notification.
- A basic understanding of the two tier fee regime.

### **2.1.4 The Data Protection Principles (20% 8/9 hours NB this is part of the 18 hours for 2.1 the Data Protection Act)**

The objective is to ensure an understanding of how the principles regulate the processing of personal data and how they are enforced, as well as an understanding of the individual principles in the light of guidance on their interpretation found in Part II of Schedule 1. Candidates will be required to show an understanding of the need to interpret and apply the principles in context.

- Introduction: how the principles regulate and how they are enforced including Information and Enforcement Notices.
- First Principle, including transparency and Schedules 2 and 3
- Second Principle

- Third Principle
- Fourth Principle
- Fifth Principle
- Sixth Principle
- Seventh Principle
- Eighth Principle, including paragraph 13 of Part II of Schedule 1 and Schedule 4

**NB First Principle above** - Candidates should appreciate the distinction between the grounds for processing in Schedules 2 and 3 and the non-disclosure exemptions. They should also have basic understanding of the law of confidence and the potential interaction with the First Principle.

### 2.1.5 Individual Rights

The objective is to ensure an understanding of the rights conferred by the Act and how they can be applied and enforced.

- Right of subject access
- Right to attempt to prevent processing likely to cause damage or distress
- Right to prevent processing for the purpose of direct marketing
- Rights in relation to automated decision taking
- Right to compensation
- Right to rectification, blocking, erasure and destruction
- Right to request s42 assessment of processing

**NB Re. subject access fees: Candidates are only expected to know that the standard fee is £10 and are not expected to know, for example, the fee regime in respect of educational records.**

### 2.1.6 Exemptions

The objective is to ensure awareness of the fact that there are exemptions from certain provisions of the Act, and knowledge and understanding of some of these and how to apply them in practice. Candidates are not expected to have a detailed knowledge of all the exemptions. The following are expected to be covered in some detail:

- Domestic Purposes
- Crime and Taxation (s29 (1), (2), and (3) only)
- Information required to be made public
- Disclosures required by law or made in connection with legal proceedings
- Confidential references
- Management forecasts and planning
- Negotiations
- Research, history and statistics
- Special purposes (s32 (1), (2) & (6) only)
- Legal professional privilege (a basic understanding of the circumstances in which this might apply only)

In addition candidates are expected to know what is meant by “the subject information provisions” and “the non-disclosure provisions”.

### 2.1.7 Offences

The objective is to ensure an awareness of the fact that there are a range of offences under the Act and of the role of the Courts as well as an appreciation of how certain specified offences apply in practice. It is not intended that candidates should have a detailed knowledge of all the offences. The candidates will be expected to cover:

- Unlawful obtaining and disclosure of personal data
- Unlawful selling of personal data

- Processing without notification
- Failure to notify changes in processing
- Failure to comply with an Enforcement Notice, an Information Notice or Special Information Notice.

## **2.2 Privacy and Electronic Communications (EC Directive) Regulations 2003 (5% 2 hours course work)**

The objective is to ensure an awareness of the relationship between the above Regulations and the Act, an awareness of the broad scope of the Regulations and a detailed understanding of the practical application of the main provisions relating to unsolicited marketing.

- Objective and broad scope
- Provisions relating to unsolicited marketing calls
- Provisions relating to unsolicited marketing faxes
- Provisions relating to unsolicited marketing emails (including SMS)

## **2.3 Associated legislation (2.5% 1 hour course work)**

The objective is to ensure a basic awareness of some other legislation which is relevant and an appreciation that data protection legislation must be considered in the context of other law.

- Computer Misuse Act 1990 – awareness of broad scope.
- Freedom of Information Act 2000 – awareness of broad scope and inter-relationship with DPA98
- Regulation of Investigatory Powers Act 2000 and The Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 – awareness of law regarding monitoring communication
- Crime and Disorder Act 1998 – awareness of power to share information
- Anti-Terrorism Crime and Security Act 2001 – awareness of power to use information without consent

## **3. Application (45% - 18 hours of course work)**

The objective is to ensure an understanding of the practical application of the Act in a range of circumstances. This will include detailed analysis of sometimes complex scenarios, and deciding how the Act applies in particular circumstances and explaining and justifying a decision taken or advice given.

### **3.1 How to comply with the Act**

- Identification of processing subject to the Act
- Notification in practice
- Using Privacy Impact Assessments
- Adopting a Privacy by Design approach
- Policies and practice to adopt to comply with the 7<sup>th</sup> Principle including when to notify a data loss
- Policies and practice to adopt for data subject access

### **3.2 Addressing scenarios in specific areas**

- Marketing
- Financial services
- Local Government
- Central Government
- Human Resource management
- Health sector

### **3.3 Data processing topics**

- Monitoring – internet, email, telephone calls and CCTV
- Use of the internet (including Electronic Commerce)
- Data matching
- Disclosure and Data sharing

The focus here is on the practical application of the Act, particularly in circumstances where this might not be clear-cut as will often be the case in real life. It is strongly recommended that case studies/scenarios and practical examples are used so that candidates become familiar with the practicalities of compliance. Compliance advice on particular topics and for specific sectors is published by the Information Commissioner. It is strongly recommended that human resource management related issues are addressed.

## **Additional Information**

### **Levels of Skill and Responsibility (SFIA Levels)**

The levels of knowledge above will enable candidates to develop the following levels of skill to be able to operate at the following levels of responsibility (as defined within the SFIA framework) within their workplace:

#### **Level 1: Follow**

Work under close supervision to perform routine activities in a structured environment. They will require assistance in resolving unexpected problems, but will be able to demonstrate an organised approach to work and learn new skills and applies newly acquired knowledge.

#### **Level 2: Assist**

Works under routine supervision and uses minor discretion in resolving problems or enquiries. Works without frequent reference to others and may have influence within their own domain. They are able to perform a range of varied work activities in a variety of structured environments and can identify and negotiate their own development opportunities. They can also monitor their own work within short time horizons and absorb technical information when it is presented systematically and apply it effectively.

#### **Level 3: Apply**

Works under general supervision and uses discretion in identifying and resolving complex problems and assignments. They usually require specific instructions with their work being reviewed at frequent milestones, but can determine when issues should be escalated to a higher level. Interacts with and influences department/project team members. In a predictable and structured environment they may supervise others. They can perform a broad range of work, sometimes complex and non-routine, in a variety of environments. They understand and use appropriate methods, tools and applications and can demonstrate an analytical and systematic approach to problem solving. They can take the initiative in identifying and negotiating appropriate development opportunities and demonstrate effective communication skills, sometimes planning, scheduling and monitoring their own work. They can absorb and apply technical information, works to required standards and understand and uses appropriate methods, tools and applications.

#### **Level 4: Enable**

Works under general direction within clear framework of accountability and can exercise substantial personal responsibility and autonomy. They can plan their own work to meet given objectives and processes and can influence their team and specialist peers internally. They can have some responsibility for the work of others and for the allocation of resources. They can make decisions which influence the success of projects and team objectives and perform a broad range of complex technical or professional work activities, in a variety of contexts. They are capable of selecting appropriately from applicable standards, methods, tools and applications and demonstrate an analytical and systematic approach to problem solving, communicating fluently orally and in writing, and can present complex technical information to both technical and non-technical audiences. They plan, schedule and monitor their work to meet time and quality targets and in accordance with relevant legislation and procedures, rapidly absorbing new technical information and applying it effectively. They have a good appreciation of the wider field of information systems, their use in relevant employment areas and how they relate to the business activities of the employer or client.

### **Level 5: Ensure and advise**

Works under broad direction, being fully accountable for their own technical work and/or project/supervisory responsibilities, receiving assignments in the form of objectives. Their work is often self-initiated and they can establish their own milestones, team objectives, and candidates responsibilities. They have significant responsibility for the work of others and for the allocation of resources, making decisions which impact on the success of assigned projects i.e. results, deadlines and budget. They can also develop business relationships with customers, perform a challenging range and variety of complex technical or professional work activities and undertake work which requires the application of fundamental principles in a wide and often unpredictable range of contexts. They can advise on the available standards, methods, tools and applications relevant to own specialism and can make correct choices from alternatives. They can also analyse, diagnose, design, plan, execute and evaluate work to time, cost and quality targets, communicating effectively, formally and informally, with colleagues, subordinates and customers. They can demonstrate leadership, mentor more junior colleagues and take the initiative in keeping their skills up to date. Takes customer requirements into account and demonstrates creativity and innovation in applying solutions for the benefit of the customer.

### **Level 6: Initiate and influence**

Have a defined authority and responsibility for a significant area of work, including technical, financial and quality aspects. They can establish organisational objectives and candidates responsibilities, being accountable for actions and decisions taken by them self and their subordinates. They can influence policy formation within their own specialism to business objectives, influencing a significant part of their own organisation and customers/suppliers and the industry at senior management level. They make decisions which impact the work of employing organisations, achievement of organisational objectives and financial performance, developing high-level relationships with customers, suppliers and industry leaders. They can perform highly complex work activities covering technical, financial and quality aspects. They contribute to the formulation of IT strategy, creatively applying a wide range of technical and/or management principles. They absorb complex technical information and communicate effectively at all levels to both technical and non-technical audiences, assesses and evaluates risk and understand the implications of new technologies. They demonstrate clear leadership and the ability to influence and persuade others, with a broad understanding of all aspects of IT and deep understanding of their own specialism(s). They take the initiative in keeping both their own and subordinates' skills up to date and to maintain an awareness of developments in the IT industry.

### **Level 7: Set strategy, inspire and mobilise**

Have the authority and responsibility for all aspects of a significant area of work, including policy formation and application. They are fully accountable for actions taken and decisions made, by both them self and their subordinates. They make decisions critical to organisational success and influence developments within the IT industry at the highest levels, advancing the knowledge and/or exploitation of IT within one or more organisations. They develop long-term strategic relationships with customers and industry leaders, leading on the formulation and application of strategy. They apply the highest level of management and leadership skills, having a deep understanding of the IT industry and the implications of emerging technologies for the wider business environment. They have a full range of strategic management and leadership skills and can understand, explain and present complex technical ideas to both technical and non-technical audiences at all levels up to the highest in a persuasive and convincing manner. They have a broad and deep IT knowledge coupled with equivalent knowledge of the activities of those businesses and other organisations that use and exploit IT. Communicates the potential impact of emerging technologies on organisations and individuals and analyses the risks of using or not using such technologies. They also assess the impact of legislation, and actively promote compliance.

## **Levels of Knowledge (K Levels)**

The following levels of knowledge shall be defined and applied for syllabus creation. Each topic in the syllabus shall be examined according to the learning objectives defined in the section devoted to that topic. Each learning objective has a level of knowledge (K level) associated with it and this K level by association defines the nature of any examination questions related to that topic.

Note that each K level subsumes lower levels. For example, a K4 level topic is one for which a candidate must be able to analyse a situation and extract relevant information. A question on a K4 topic could be at any level up to and including K4. As an example, a scenario requiring a candidate to analyse a scenario and select the best risk identification method would be at K4, but questions could also be asked about this topic at K3 and a question at K3 for this topic might require a candidate to apply one of the risk identification methods to a situation.

### **Level 1: Remember (K1)**

The candidate should be able to recognise, remember and recall a term or concept but not necessarily be able to use or explain. Typical questions would use: define, duplicate, list, memorise, recall, repeat, reproduce, state.

### **Level 2: Understand (K2)**

The candidate should be able to explain a topic or classify information or make comparisons. The candidate should be able to explain ideas or concepts. Typical questions would use: classify, describe, discuss, explain, identify, locate, recognise, report, select, translate, paraphrase.

### **Level 3: Apply (K3)**

The candidate should be able apply a topic in a practical setting. The candidate should be able to use the information in a new way. Typical questions would use: choose, demonstrate, employ, illustrate, interpret, operate, schedule, sketch, solve, use, write.

### **Level 4: Analyse (K4)**

The candidate should be able to distinguish/separate information related to a concept or technique into its constituent parts for better understanding, and can distinguish between facts and inferences. Typical questions would use: appraise, compare, contrast, criticise, differentiate, discriminate, distinguish, examiner, question, test.

### **Level 5: Synthesise (K5)**

The candidate should be able to justify a decision and can identify and build patterns in facts and information related to a concept or technique, they can create new meaning or structure from parts of a concept. Typical questions would use: appraise, argue, defend, judge, select, support, value, evaluate.

### **Level 6: Evaluate (K6)**

The candidate should be able to provide a new point of view and can judge the value of information and decide on its applicability in a given situation. Typical questions would use: assemble, contract, create, design, develop, formulate, write. Learning objectives are given indicators from K1-K6. These are based on Bloom's taxonomy of knowledge in the cognitive domain (ref Taxonomy of Educational Objectives, Handbook 1 – The Cognitive Domain, Bloom et al., New York 1956), and can be broadly interpreted as follows: K1 – Remember; K2 – Understand; K3 –

Apply; K4 – Analyse; K5 – Synthesise; K6 – Evaluate. Bloom’s taxonomy is explained in greater detail in Section 5.1. All topics shall have learning objectives associated with them, each of which has an associated K level. The language used must, as far as possible, mirror the language used in defining Bloom’s taxonomy to provide candidates with consistent pointers to the expected level of knowledge and a consistent way of expressing that level in words.

This course will provide candidates with the levels of knowledge highlighted within the following table, enabling them to develop the skills to operate at the levels of responsibility indicated. The levels of knowledge, skill and responsibility are explained in the following text:

Level	Levels of knowledge	Levels of skill and responsibility
7		Set strategy, inspire and mobilise
6	Evaluate	Initiate and influence
5	Synthesise	Ensure and advise
4	Analyse	Enable
3	Apply	Apply
2	Understand	Assist
1	Remember	Follow

### Examination Details

Type:	20% multiple choice; 40% short bullet point answers; 40% discursive essays.
Duration:	3 hours. Candidates who have a recognised disability may request extra time as well as candidates sitting the examination in a language other than their native language. This must also be included in this section. Candidates may take in a <b>paper</b> dictionary if their first language is not English but this will need to be checked by the invigilator prior to the examination.
Pre-Requisite for course and/or exam:	70% attendance of accredited course unless special dispensation granted.
Invigilated/Proctored:	Invigilated.
Closed Book (No reading materials allowed into the examination room).	Closed book.
Learning Hours	40 hours of direct contact training time.
Pass Mark	50/100
Distinction Score	80/100
Delivery:	Usually classroom based tuition but no fundamental objection to the use of distance learning mechanisms.

### Trainer Qualification Criteria

Criteria:	Trainers must usually hold the ISEB Data Protection Certificate though dispensation can be given. All Course Directors and trainers must be individually accredited.
-----------	--

### Classroom Size

Trainer to candidate ratio:	1:16 ratio
-----------------------------	------------