



**Certificate in Data Protection**  
**Syllabus (Version 5.6)**

## **ISEB Syllabus for the Certificate in Data Protection (Version 5.6)**

### **Introduction**

There is a need to provide adequate training on the Data Protection Act 1998 "the Act" and its implications for both organisations and individuals. There are important differences between the Act and its predecessor, the Data Protection Act 1984. In particular, the Act contains important new obligations in relation to manual records and transborder data flows, a new notification system and amended principles. It is important to understand the Act in the European context.

Those experienced in data protection issues, as well as those new to the subject, need to be trained so that their organisations are confident that legal compliance is continually addressed. It is necessary to identify issues requiring expert data protection advice in good time in order that organisational reputation and credibility are enhanced through relevant data protection policies and procedures.

The ISEB Certificate in Data Protection provides a qualification that demonstrates competence for those with some data protection responsibilities within their organisations. It also provides an effective conversion route for those experienced practitioners needing to update their knowledge of and practice under the 1984 Data Protection Act. It is recognised that individuals with overall responsibility for data protection compliance within an organisation, whilst benefiting from the qualification, would need to pursue their studies further for a fuller understanding of the more intricate issues of the legislation.

### **Aim**

The aim of the syllabus is to promote an understanding of how the data protection principles work rather than simply focusing on the mechanics of regulation. The syllabus places the Act in the context of human rights and promotes good practice within organisations. On attaining the certificate, award holders will possess:

- an appreciation of the broader context of the Act.
- an understanding of the way in which the Act and the Privacy and Electronic Communications (EC Directive) Regulations 2003 work
- a broad understanding of the way associated legislation relates to the Act
- an understanding of what has to be done to achieve compliance
- a recognised qualification in data protection

## Structure

The syllabus comprises five parts:

- 1 Context** - this will address the origins of and reasons for the Act together with consideration of privacy in general.
- 2a Law – Data Protection Act** - this will address the main concepts and elements of the Act and subordinate legislation.
- 2b Law – Privacy and Electronic Communications (EC Directive) Regulations 2003** - this will address the main concepts and elements of the Regulations and their relationship to the Act.
- 2c Law – Associated Legislation** - this will address other associated legislation
- 3 Application** - this will consider how compliance is achieved and how the Act works in practice.

## Syllabus

### Part 1 Context - 1 hour of course work

The objective is to ensure an understanding of the purpose of the legislation.

#### A What is privacy

- A1 An understanding of the context of the right to private and family life and an awareness of the relevance of confidentiality and privacy in relation to data protection and telecommunications legislation.
- A2 European Convention on Human Rights and Fundamental Freedoms, UK Human Rights Act (relating to information)

#### B History and origin of data protection legislation in the UK

- B1 OECD Guidelines on the Protection of Privacy and Transborder Flows of personal Data, OECD 1980.
- B2 Council of Europe Convention 108, 1981
- B3 The Data Protection Act, 1984
- B4 European Data Protection Directive 95/46/EC.
- B5 Telecommunications Directive 97/66/EC, Privacy & Electronic Communications Directive 2002/58/EC, and subsequent revisions of the latter.

## Explanatory note

It is recommended that only one hour of study is spent on this topic. Clearly this depth of study can only serve as an overview of the topic. However it should develop an appreciation that privacy and data protection is an area far wider than the Act, and thus place the Act in context. Course material for this part should draw upon the more general items included in the bibliography for course providers.

## **Part 2a, 2b & 2c Law - 21 hours of course work**

As this is a basic certificate course and only 21 hours are allocated for instruction on this part of the syllabus, it would be unrealistic and unfair to expect a detailed knowledge of, and understanding of, the whole Act. A detailed knowledge is not expected of the provisions in relation to the special purposes.

### **Part 2a - Data Protection Act - 17 hours course work**

#### **A The Definitions**

The objective is to ensure an understanding of the major definitions in the Act in order to identify what information and processing activities are subject to the Act.

- A1 Data including Relevant Filing System, Accessible Records and category (e) unstructured Data
- A2 Personal Data
- A3 Processing
- A4 Data Subject
- A5 Data Controller
- A6 Data Processor
- A7 Recipient
- A8 Third Party
- A9 Sensitive Personal Data
- A10 The Special Purposes

#### **Explanatory note**

Though candidates are expected to be aware that the FOI ACT 2000 created a new category of Data, category (e) data, they are not expected to understand the implications for this in respect of the section 7 right of subject access. Candidates are not required to know the section 33 (A)(1) and section 33 (A)(2) exemptions.

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, 44, 45 and 46 of the Act.

#### **B Role of the Information Commissioner**

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

- B1 Enforcement (Including the roles of the Information Tribunal & of the Courts)
- B2 Assessment
- B3 Codes of Practice

#### **Explanatory Note**

Changes in legislation within the Criminal Justice and Immigration Act 2008 will be included once Parliament has finalised the detail of these powers.

## **C Notification**

The objective is to ensure a broad, but not detailed, understanding of the notification scheme.

- C1 Information to be notified and the public register
- C2 Awareness of the existence of any exemptions from notification
- C3 Awareness of assessable processing provisions

## **D The Data Protection Principles**

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 a reasonable understanding of the individual principles in the light of the guidance on their interpretation provided in Part II of Schedule 1. Candidates will be required to show an understanding of the need to interpret the principles in context.

- D1 Introduction: how the principles regulate and how they are enforced including Information Notices and Enforcement Notices
- D2 First Principle, including Schedule 2 and Schedule 3 and informing data subjects.
- D3 Second Principle
- D4 Third Principle
- D5 Fourth Principle
- D6 Fifth Principle
- D7 Sixth Principle
- D8 Seventh Principle
- D9 Eighth Principle, including paragraph 13 of Part II of Schedule 1 and Schedule 4

## **Explanatory note**

It is recommended that 8-9 hours of study are spent on Section D. Students will be expected to have an understanding of the limitations on the powers of public bodies in respect of the application of the First and Second Principles. Candidates should appreciate the distinction between the grounds for processing provided in Schedules 2 and 3 and the non-disclosure exemptions.

## **E Individual Rights**

The objective is to ensure an understanding of the individual rights conferred by the Act and the manner by which these may be enforced.

- E1 Right of Subject Access
- E2 Right to prevent processing likely to cause damage or distress
- E3 Right to prevent processing for purpose of direct marketing
- E4 Rights in relation to automated decision taking
- E5 Right to compensation
- E6 Rectification, blocking, erasure and destruction
- E7 Requests for assessment

## **F Exemptions**

The objective is to ensure an awareness of the fact that there are exemptions from some or all of the provisions of the Act. It is not intended that students should have a detailed knowledge of all the exemptions. The generally applicable sections of the following are expected to be covered in some detail:

- F1 Domestic Purposes (Personal, Family or Household Affairs) Exemptions
- F2 Crime and taxation exemptions
- F3 Information required to be made public
- F4 Disclosures required by law or made in connection with legal proceedings.
- F5 Confidential References
- F6 Management Forecasts/Planning
- F7 Negotiations
- F8 Research, History and Statistics

## **G Offences**

The objective is to ensure an awareness of the fact that there is a range of offences under the Act and also of the role of the courts. It is not intended that students should have a detailed knowledge of all of the offences and enforcement procedures. The following are expected to be covered:

- G1 Unlawful obtaining and disclosure of personal data
- G2 Unlawful selling of personal data
- G3 Enforced subject access
- G4 Processing without notification
- G5 Failure to notify changes in processing
- G6 Failure to comply with an Enforcement Notice, an Information Notice or Special Information Notice

**Part 2b – Privacy and Electronic Communications (EC Directive) Regulations  
2003 - 3 hours course work**

The objective is to ensure an awareness of the relationship between the above Regulations and the Act, and an understanding of their scope and their main provisions.

- A1 Objective and scope
- A2 Restrictions on processing traffic and billing data
- A3 Provisions relating to calling line and connected line identification excluding exemptions
- A4 Individual subscriber rights in respect of directory entries
- A5 Provisions relating to unsolicited marketing calls
- A6 Provisions relating to unsolicited marketing faxes
- A7 Provisions relating to unsolicited marketing emails (including SMS)

**Part 2c - Associated Legislation - 1 hour course work**

The objective is to ensure an awareness of some of the other associated legislation which is relevant to the Act

- A1 **The Computer Misuse Act, 1990** - Awareness of its relationship with the Act, broad scope and outline of main provisions.
- A2 **Freedom of Information Act, 2000** - Awareness of its existence and the impact in outline on the Act.
- A3 **Regulation of Investigatory Powers Act, 2000 and The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000** - Awareness of monitoring communications
- A4 **Crime and Disorder Act 1998** - Awareness of the power to share information
- A5 **Anti-Terrorism Crime and Security Act 2001** - Awareness of the power to use information without consent
- A6 **Defamation Act 1996** - Awareness of liability for the information which may be defamatory

**Explanatory note**

This part is intended to provide students with an awareness that Data Protection legislation must be considered in the context of other law. Given the time of study available an in-depth knowledge is not expected. Candidates are only expected to have a broad grasp of the relationship between these Acts and the Data Protection Act 1998.

### **Part 3 Application - 18 hours of course work**

The objective is to ensure an understanding of the concept of “compliance” within a range of work settings covering both the public and private sectors and in relation to a number of relevant issues.

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

- A1 Identification of processing within the scope of the Act
- A2 Notification in practice
- A3 Policies and practice to adopt for using information systems
- A4 Policies and practice to adopt for developing information systems
- A5 Policies and practice to adopt for keeping information safe
- A6 Policies and practice to adopt for data subject access

#### **B Case situations in specific functions**

- B1 Marketing
- B2 Financial services
- B3 Local authorities
- B4 Other public authorities
- B5 Human resource management

#### **C Consideration of data processing topics**

- C1 Monitoring internet, email, intranet, telephone calls and CCTV
- C2 Smart cards
- C3 Electronic commerce
- C4 Data matching
- C5 Data sharing
- C6 Data access
- C7 Data encryption

#### **Explanatory note**

This part provides a more practical perspective on the Act. Students should understand how to undertake the necessary tasks to achieve compliance. It is recommended that this part of the syllabus is studied with the use of case studies and practical examples so students become familiar with effective strategies for dealing with everyday data protection issues. Guidance on specific sectors, and data processing environments, applications and techniques is available from the Information Commissioner. Where appropriate, case situations used on a given course could focus primarily on a specific sector with limited cover of other sectors. It is strongly recommended that human resource / personnel related data protection issues are covered on all courses.

## Assessment

This will be by a three-hour examination comprising three sections. The format of the examination is as follows with a balance of questions across the syllabus:

- Section A
  - 20 multiple choice questions (1 mark each) on Part 1 Context and Part 2 Law
  - all questions to be attempted
  - 20 marks available
- Section B
  - 8 questions (5 marks each) requiring short answers - on Part 1 Context, Part 2 Law and/or combined Part 2 Law and Part 3 Application
  - all questions to be attempted
  - 40 marks available
- Section C
  - 6 questions requiring longer discursive responses - on combined Part 1 Context, Part 2 Law and Part 3 Application;
  - questions will be phrased in such a way that candidates will be encouraged to draw upon their own work experiences or their general knowledge as members of society in addition to the specialist knowledge gained through the course on Data Protection
  - 4 questions to be attempted (10 marks each)
  - 40 marks available