Practitioner Certificate in Data Protection

Syllabus

The Syllabus for the Practitioner Certificate in Data Protection Programme covers all practical aspects of data protection law and practice in the United Kingdom. Completion of the Programme, including passing the Examination, demonstrates that the candidate has achieved a thorough understanding of the practical application of data protection legal requirements.

Part 1 of the Syllabus (80% of the total), the Core Elements, is composed of three sections:

- Fundamentals
- Subject Access Requests
- Data Security

Part 2 of the Syllabus (20% of the total), the Elective Element, allows candidates to choose one of the following subject areas:

- Data Protection in the Workplace
- International Transfers
- FOI & Data Protection

The content of each of the elements of the Syllabus is set out below, including percentages showing the proportion of the whole syllabus attributed to the specific elements.

Part 1

Fundamentals (40%)

- when and how data protection law applies to organisations
- the main definitions – ‘personal data’, ‘data subject’, ‘data controller’, ‘data processor’
- the distinction between electronic and manual records
- the requirements for using ‘sensitive personal data’
- individuals’ rights – subject access, cessation of direct marketing, automated decisions
- data retention – the restrictions on keeping data, and how to establish a retention schedule
- transferring data to third parties – the legal requirements for transferring data between organisations, including responding to requests for personal data from persons other than the data subject
- the main exemptions in the DPA - section 29 (crime and tax) and section 35(1) (disclosures required by law) and section 35(2) (legal professional privilege) – and the distinction between the ‘subject information provisions’ and the non-disclosure provisions’
- criminal offences – an introduction to the main offences in the DPA, including potential penalties
- the legal requirements for gathering information for marketing, including the drafting of opt-out and opt-in clauses
- what types of communication constitute ‘marketing’
- how the choice of media (email, text message, fax, telephone, post) affects the conduct of the marketing campaign
- the distinction between targeting corporate entities and individuals for marketing purposes
- the purpose and effect of opt-out and opt-in clauses, including how to draft such clauses to achieve desired outcomes

- the requirements of the Privacy & Electronic Communications (EC Directive) Regulations 2003, including an analysis of the exemption from the opt-in requirement for email marketing campaigns
- the implications of using cookies and other tracking technologies on websites
- an introduction to the restriction on cross border data transfers methodology involved in sending personal information abroad
- the legal requirements for outsourcing personal data processing operations (using data processors and the engagement of sub-processors)
- the role of the Information Commissioner's Office – compliance and enforcement, including powers of investigation and the power to impose fines organisations for breaches
- Information and Enforcement Notices
- the Notification system including what and how to notify, plus an understanding of the offences associated with Notification
- data destruction – methods to ensure lawful and secure destruction
- risk assessments – the basics of when and how to carry out a risk assessment
- associated legislation - an introduction to Human Rights law and Freedom of Information law

Subject Access Requests (20%)

- determining whether a valid request has been made for subject access
- liaising with the applicant to clarify the request
- time limits and fees
- analysing whether any manual (paper) records fall within the request
- setting parameters for the search for information and collating the results
- establishing whether the retrieved information is personal data
- dealing with third party information, including applying the reasonableness test and handling redaction operations
- applying relevant exemptions, including confidential references, management forecasting and negotiations
- the operation of the 'disproportionate effort' exemption from the requirement to supply data in permanent form
- presenting the response to the applicant
- managing dissatisfied recipients
- role of the Information Commissioner's Office
- an introduction to the relationship of subject access with the right to request information under the Freedom of Information Act 2000
- ensuring appropriate staff awareness and training
- establishing a policy for handling subject access requests

Data Security (20%)

- detailed analysis of the practical application of the Seventh Data Protection Principle
- relevant guidance from the Information Commissioner's Office
- the law of confidentiality and its relevance to data security
- applicable regulatory regimes including guidance from the Financial Services Authority
- data security implications of using external contractors and outsourced service providers
- the Information Commissioner's new power to issue Monetary Penalty Notices and other legal and commercial consequences of data security breaches
- managing a data security breach – law and best practice
- Information security standards, including ISO27001
- encryption of portable electronic devices
- staff vetting and testing
- security breaches: informing individuals and the Information Commissioner
- confinement strategies

Part 2

Candidates must choose one of the following three Elective Elements (20% each)

Data Protection in the Workplace ('the Staff Data Elective')

- obtaining, using and managing staff information
- ensuring that the recruitment and selection process meets the legal requirements, including the content of application forms, pre-employment vetting, criminal records, medical checks and the interview process
- retaining staff records, including setting appropriate periods of time for keeping information
- dealing with information requests from staff
- disclosing staff information to outside third parties
- references and the rights of ex-members of staff
- monitoring staff activities and communications, including using private detectives, CCTV cameras and website monitoring technologies
- handling relevant sensitive information such as health and sickness records and medical data
- how to handle mergers, acquisitions and restructuring
- outsourcing functions to third party providers
- the Information Commissioner's Employment Code
- the role of the Information Commissioner and an introduction to handling an investigation
- by the Commissioner

Transferring Data Abroad ('the International Elective')

- analysis of the restrictions in the Eighth Data Protection Principle including what amounts to a 'transfer'
- consideration of the distinction between 'safe' and 'non-safe' countries
- detailed consideration of the derogations and exemptions, including consent, contractual necessity, 'model contracts', binding corporate rules and 'safe harbor'
- when to consider making an 'assessment of adequacy'
- determining the most practical and cost effective method to achieve data export goals
- security implications of using foreign service providers such as offshore call centres

FOI and Data Protection Working Together – ('the FOI Elective')

- determining what is personal data in the context of FOI requests, including relevant guidance from the Information Commissioner's Office
- determining whether a request should be dealt with under the Data Protection Act 1998, the Freedom of Information Act 2000 ('FOIA'), or the Environmental Information Regulations 2004
- interpretation and practical application of section 40, FOIA
- the legal principles governing access to third party personal data
- applying relevant FOIA exemptions
- disclosing staff information to outside third parties
- analysing the practical implications of key decisions of the Information Commissioner and Tribunal
- disclosing third party data of professionals in the fields of health, education and social work