Certified Data Protection Practitioner in Education/Foundation (CDPPE/F)

Syllabus and Examination Guidance V1.0

Table of Contents

1. Introduction to the Certified Data Protection Practitioner in Education ("CDPPE/F")

A three-day training course leading to a qualification, specifically designed for Data Protection Officers (DPOs) or data protection leads working in UK schools (nurseries, primary and secondary schools, sixth form colleges etc.), colleges of further education and higher education. The syllabus identifies, and deals with, where data protection law differs between a public authority and an independent educational establishment.

The scope of the course is UK data protection law specifically in the context of its application to educational establishments operating within the UK.

2. Training eligibility criteria

The Certified Data Protection Practitioner in Education/Foundation (CDPPE/F) course is aimed at Data Protection Officers, data protection leads and anyone who has to deal with data protection compliance in an education setting. i.e., nurseries, schools, colleges, and universities. The content is geared to the processing of personal data by educational establishments whether they are a public authority or not.

Where the law operates differently between a public authority and a non-public authority, the trainer will explain the differences. For example, because the range of manual personal data is wider for a public authority than for a non-public authority, a public authority educational establishment dealing with a Subject Access Request may be required to search for personal data held in certain unstructured paper records.

No previous knowledge of, or practice in, data protection law is required.

Delegates who have successfully completed the Foundation course can progress to the Certified Data Protection Practitioner in Education/Advanced course.

3. What will you learn?

After attending the course and successfully completing the examination you will:

- ***Hold a qualification in data protection*** – the Certified Data Protection Practitioner in Education/Foundation. This will help demonstrate to employers that you have a robust knowledge of data protection law and its application in an education setting.

- ***Be able to assess the output, quality, and effectiveness of any outsourced Data Protection Officer service*** that your organisation procures. You will also be able to assess, and monitor, with confidence, the reliability of DPO services going forward.

- You will have the necessary skills to help ***perform the tasks of a DPO or Senior Responsible Individual (SRI)****

    - **The legislative changes proposed by Government in the Data Protection and Digital Information (No. 2) Bill include replacing a DPO with a requirement to appoint a Senior Responsible Individual (SRI) from within existing senior management of the educational establishment.*

- You will be able to ***demonstrate knowledge in the following areas*** and be able to apply that knowledge in an education-specific setting:

  Read the full syllabus in ***Appendix 1.***

    - The ***Data Protection legal landscape*** in the UK (including the UK GDPR, Data Protection Act 2018);
    - Understand ***essential terminology***, data protection concepts;
    - Know where the main ***data protection "trigger points" lie in an educational establishment.*** e.g., use of personal devices, remote working, data sharing, international transfers, use of student images, data sharing, EdTech, and data breaches;
    - *Understand* ***an educational establishment's main data protection obligations.*** e.g., compliance with the data protection principles, record keeping and breach

reporting requirements, duty to pay the Controller's fee, and compliance with individual rights including Subject Access Requests (SARs);

- *Understand* ***the requirement to have a lawful basis for the processing***;
- Understand ***how to comply with the data protection principles***; ***when to conduct a Legitimate Interest Assessment*** (***LIA***); ***when to rely on "consent"*** and when not to rely on "consent" and ***the requirements of legally valid consent***;
- Understand ***how to draft a privacy notice*** and what it must contain;
- *Understand* ***how to process special categories of personal data lawfully*** under UK GDPR and the Data Protection Act 2018, E.g., in the context of SEND, Exam Access Arrangement (EAA) information;
- *Understand* the principle requiring you to take technical and organisational ***security measures to protect personal data*** and ***what measures you are expected to implement within your setting.*** E.g., when working in an office, classroom, remotely, on the move or from home;
- Understand how to comply with ***the Accountability Principle*** in order to be able to demonstrate compliance, including ***which accountability measures are obligatory*** and the circumstances under which they are obligatory, such as data protection policies and the appointment of a DPO, and which measures are optional? (Article 24/25 UK GDPR);
- How and when to carry out a ***Data Protection Impact Assessment*** (DPIA);
- Understand the ***requirements*** under UK GDPR ***relating to staff data protection training and data protection policies***;
- Understand the different ***individual legal rights***; ***how to handle a Subject Access Request*** including when you can refuse one; understanding the ***exemptions*** from the right of subject access that typically apply to educational establishments;
- *Understand* ***when you are required to appoint a DPO, maintain a Record of Processing Activities (ROPA) and pay the annual Controller fee***;
- Understand the ***role and enforcement powers of the ICO***, aspects of the ICO's Regulatory Action Policy (RAP); certain ***criminal offences*** including the offence of unlawful obtaining of personal data; offence of re-identification of de-identified personal data; offence of alteration, blocking, erasing etc. of personal data following a request such as a SAR; penalties for breaches;
- ***Data Subject's remedies*** for infringements;
- Understand and overcome the challenges of ***using student images lawfully***. E.g., lawful use of student images on your website, social networking platforms and in printed publicity;
- Understand the rules relating to ***data sharing with third parties***. E.g., disclosures to other parents, the local authority, police, Children's Services/Child Protection, service providers such as cloud service providers;
- Understand the specific data protection ***compliance issues around using Edtech*** including the UK GDPR rule relating to contracts between Controllers and Processors;

- Understand about the ***Age-Appropriate Design Code (or Children's Code)*** in the context of Edtech; understanding if and when, the Code applies to you or to your service providers;
- Understand the data protection rule that is engaged (and how to comply) when ***processing the personal data of a child under the age of 13 years, on the lawful basis of consent, in the context of an Internet Society Service (ISS)***;
- ***Learn how to recognise, handle, and prevent personal data breaches in an educational establishment;*** know when to report a breach to the ICO and affected individuals; what to include in a notification to comply with the law but minimise the risk of a civil claim against you;
- Understand the ***basic rules relating to international transfers of Personal Data from the UK to other countries*** and the typical options for an educational establishment to consider, to ensure that a transfer complies with UK GDPR rules relating to international transfers. The course includes a high-level review of the latest developments including the EU-US Data Privacy Framework and the UK Extension to it, Standard Data Protection Clauses and when to carry out a Transfer Risk Assessment (TRA);
- Understand the ***data protection risks related to remote working and working from personal devices and how to mitigate those risks***;
- Understand the ***data protection considerations and risks of using Artificial Intelligence (AI) and Generative AI for teaching and learning, HR and how to mitigate those risks***; The DoE's Policy Paper "Generative Artificial Intelligence (AI) in Education"; Understand the AI regulatory landscape;
- ***Horizon scanning: A review of the potential changes to UK Data Protection law including the Data Protection Digital Information Bill and a summary of how the changes will affect educational establishments***;
- Understand ***how to achieve and maintain a culture of compliance in an education setting***. Understand the challenges and how to overcome them.

4. Certification

The examination consists of 50 multi choice questions and lasts 90 minutes. Candidates who sit and pass the examination will attain certification. This includes a personal digital certificate which they can download.

Further information about the format of the examination is set out in Section 6. A number of sample questions are provided in Appendix 2. A larger number of example exam questions is available upon request for potential exam delegates working within educational establishments.

The training and examination is provided by Tenjin Limited in association with Amberhawk Training Limited ("Amberhawk"), a renowned Information Law training company founded in 2008 and accredited by the British Computer Society. This means that the training content and syllabus has been reviewed by experts at Amberhawk Training Limited, who also have a role in setting the exam, the syllabus and ensuring exam standards.

Please note, the certification is not regulated by Ofqual, Qualification Wales, CCEA or SQA.

5. Other courses related to the CDPPE/F

Delegates who have successfully completed the Certified Data Protection Practitioner in Education/Foundation ("CDPPE/F") may then go on to take the Certified Data Protection Practitioner in Education/Advanced ("CDPPE/A").

The Advanced course covers subjects from the Foundation to a deeper and more detailed level. Examples of topics covered in the Advanced course include:

- Subject Access Requests (SARs) made in the context of legal claims, litigation, exclusions, allegations of bullying, Employment Tribunal hearings or internal Grievance and Disciplinary matters or Freedom of Information requests;
- SARs made in conjunction with the exercise of other rights such as a request for erasure of personal data;
- Requests for information containing Education Data, Health Data and Social work data are covered in practical and closer detail;
- Claiming an extension of time to deal with a request on the ground of complexity;
- Refusal of a request on the grounds of "manifestly unfounded" and "manifestly excessive".
- Processing Biometric data and Facial Recognition Technology (FRT);
- Data protection in an HR context;
- Data protection compliance when using Artificial Intelligence in an educational establishment;
- Handling a personal data breach in detail including how to draft a notification to impacted data subjects and a notification to the ICO;
- International data transfers update;
- Cookie compliance;
- Compliant direct marketing and fundraising; The Advanced course covers the relevant aspects of both UK GDPR and the Privacy and Electronic Communications Regulations 2003 (PECR). This is relevant to communications with Alumni, fundraising, direct marketing including practices such as wealth screening, profiling, lead generation, database cleansing, data matching and social networking;

- Horizon scanning; preparing for the Data Protection and Digital Information Bill. What changes are on the horizon and how should we prepare?
- Data sharing advanced workshop scenarios include the following scenarios: data sharing in the context of mergers and acquisitions, sharing children's data with other professionals, reviewing a sample data processing agreement and data sharing agreement;
- International transfers of personal data.

Alternatively, those who have several years' experience working in data protection within an education establishment and already hold a data protection qualification may feel able to bypass the CDPPE/F and go straight to the CDPPE/A. However, we recommend that all candidates take the Foundation Course and exam before progressing to the Advanced Course and exam.

6. Examination Format

The 90-minute computer-based exam (closed book) is optional but must be passed in order to achieve certified status.

The exam consists of 50 multi-choice questions. In order to pass the exam, you need to score 65% or above. This equates to 33 marks out of 50 or above.

Pass: (33/50) Candidates who score 65% or above attain a Pass.

Candidates who score under 65% (33/50) will not pass. However, they are eligible to re-sit the examination up to a maximum of TWO more times, without having to take the course again. There is a small re-sit examination fee payable to cover examination costs.

Exam Format

The format of the CDPPE/F examination consists of 50 multi-choice questions. Each question carries 1 mark. The first 40 questions are regular multi-choice questions. The last 10 multi-choice questions relate to TWO scenario-based questions; each scenario-based question has 5 multi- choice questions.

The examination is sat remotely from your computer but with a human proctor. Candidates are sent simple instructions in advance so they can familiarise themselves with the procedure and are comfortable with the arrangements.

Candidates are required to attend a brief practice tutorial and system check in advance of their examination. The purpose of this is multi – functional; it allows candidates to meet a remote exam invigilator, familiarise themselves with the exam online environment and, at the same time, have a go at answering some online questions.

Tenjin understands that some candidates have a disability, special education need, illness or temporary physical impairment (“an impairment”) and will require special arrangements and/or a reasonable adjustment to be made to facilitate their access to the examination. Tenjin has a statutory obligation to provide equal access to its examinations and, in some cases, to make a reasonable adjustment. If you suffer from an impairment, you may also be entitled to access arrangements such as extra time. For further information,

please refer to our Exam Access Arrangements Policy in the document: "***Everything You Need to Know about taking your Examination"*** Click here.

To understand more about the online exam format, minimum system requirements and the exam environment, please refer to our document: "***Everything You Need to Know about taking your Examination"*** Click here.

Sample Examination Questions: To view some CDPPE/F sample exam questions (SEE APPENDIX 2).

7. More details about our courses and booking a course.

Delegates must attend the training course before sitting the examination. There is no direct entry to the examination currently available.

Training is provided by Tenjin Limited. It is currently only available live via MS teams. The sessions are remote classroom-based and lawyer-led.

The training content and syllabus has been reviewed by experts at Amberhawk Training Limited, who also have a role in setting the exam, and ensuring exam standards.

Delegates can choose to attend group sessions which are advertised on Tenjin's website here. If this is your preference, please select "Option 1 – Public Virtual Classroom" on the online Booking Form.

Alternatively, delegates can choose to book a private session for themselves or a group from the same organisation via the Tenjin website here. If this is your preference, select "Option 2 – In-House Exclusive" on the Booking Form.

If you are booking a private session for yourself or a group from your organisation, you may be able to organise a face to face training. Please contact us separately to discuss this.

8. Recommended reading sources.

Tenjin provides delegates with key statutes on joining the course. However, delegates are reminded that legislation, guidance, codes of conduct etc. are not static and will change over time. You should therefore ensure that your sources are always up to date, especially if relying on them for your examination or preparing advice for others.

UK Data Protection Act 2018 is available here:
https://www.legislation.gov.uk/ukpga/2018/12/contents

The UK GDPR is available here
https://www.legislation.gov.uk/eur/2016/679/contents

Note: With the above link, if you choose ***"Original (as enacted)"***, you will see the pre-Brexit GDPR or Data Protection Act 2018.

If you choose, **"Latest available (Revised)",** you will see the latest post-Brexit version of the UK GDPR and Data Protection Act 2018.

ICO Data Sharing Code of Practice is available here

ICO Age-Appropriate Design Code is available here
(https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf)

ICO guidance on Artificial Intelligence (AI) and Data Protection is available here

Guidance on AI and data protection | ICO

ICO and Data Protection Tool Kit is here

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/ai-and-data-protection-risk-toolkit/

The Information Commissioner's Office (ICO) publishes a variety of guidance, and Codes of Practice. Their website can be accessed here.

9. Copyright Notice and Disclaimer

APPENDIX 1. DETAILED SPECIFICATION OF THE CDPPE/F Syllabus

If you would prefer to read a briefer, "light touch" document please go to Section 3 above "What will you learn?"

Section A: UK Data protection legislative framework

Part 1: Data protection legal landscape in the UK:

- The General Data Protection Regulation (GDPR) (EU) 2016/679 ("EU GDPR");
- UK GDPR and an overview of certain related Recitals;
- Data Protection Act 2018 ("DPA 2018");
- An overview of European Directive 2002/58/EC; The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) (PECR); PECR is identified but not examinable;
- The Data Protection and Digital Information (No.2) Bill ("DPDI2") is identified from a horizon scanning perspective but not examinable;
- Territorial scope of UK GDPR; Article 3 UK GDPR. Territorial scope of UK GDPR to controllers and processors "established" and "not established" in the UK. How this aligns with the territorial scope of EU GDPR;
- The purpose of data protection regulation and why it has value. How data protection regulation operates protects personal data.

Part 2: Essential terminology:

- Candidates will learn the following terminology: Personal Data; Special Categories of Personal Data; Criminal Offence Data; Filing System; Processing; Controller; Processor; Joint Controller; Data Subject; Unstructured manual records; Pseudonymous and anonymous data.

Part 3: Data protection "trigger points" in an educational establishment: i.e., scenarios where data protection compliance issues typically arise:

- A high-level review of the main data protection trigger points in an educational establishment. E.g., staff processing personal data on personally owned devices, staff working remotely, data sharing, EdTech, managing data breaches, lawful use of student images and compliance with individual data rights.

Part 4: An educational establishment's main protection obligations as a controller; an overview:

- Overview of an education establishment's main obligations as a Controller, followed by a more detailed look at most of those obligations.
- Compliance with the data protection principles;
- Handling personal data in line with individual legal rights;
- Designation of a DPO; maintaining a record of processing activities (ROPA); paying the annual Controller fee;
- Compliance with the UK GDPR rules relating to contracts between Controllers and Processors (Article 28 UK GDPR);
- Compliance with the rules relating to data sharing. Note: Data sharing between Joint Controllers is not examinable in the CDPPE/F. They are covered in more detail in the Advanced course);
- Data breach handling including mandatory reporting of certain types of personal data breach to the ICO and data subjects;
- Transfers to a third country only where privacy is protected and in compliance with the UK GDPR rules relating to international transfers. (Examinable at a high level only in the CDPPE/F).

Part 4A: Complying with the Data Protection Principles:

- Overview of all 7 data protection principles in Article 5. Lessons are illustrated using education-specific examples of how to comply and non-compliance. Although all 7 data protection principles are covered in the Foundation course, the following principles are covered in more granular detail. *
- ****Principle 1*** **("lawfulness, fairness and transparency")** in detail:
  - Understanding the requirement to have a lawful basis to process personal data from Article 6 UK GDPR; Exploring the different lawful bases for processing under Article 6 UK GDPR;
  - How to meet the threshold for legally valid "consent"; when it is inappropriate to rely on "consent"; drafting compliant consent mechanisms;
  - Relying on the legal bases of "contract", "legal obligation", "vital interests" and public task";
  - Relying on "legitimate interests" as a lawful basis; conducting a Legitimate Interests Assessment (LIA);
  - Lawful processing of special categories of personal data under UK GDPR and DPA 2018;
    - The conditions permitted for processing special categories of personal data under Article 9 UK GDPR;
    - Candidates will learn which of the Article 9 conditions for processing special category data require additional conditions and safeguards from Schedule 1, Part 1, DPA 2018 or Schedule 2, Part 1 DPA 2018;

- Candidates will learn which conditions under the DPA 2018 trigger the requirement to have an Appropriate Policy Document (APD) (Schedule 1, Part 4 DPA 2018) and learn what an APD must contain;
- Consideration of which Article 6 lawful base typically "pairs" with which Article 9 condition;
- The lawful processing of criminal offence data is not covered in the Foundation qualification and is not examinable;

  - Fair and transparent processing. What is meant by fair processing? What is meant by transparent processing?

- *__Principle 6__ **("The Integrity and Confidentiality Principle")** in detail;
  - Understand the principle requiring you to take technical and organisational security measures to protect personal data;
  - Examples of physical, technical, and organisational measures which can be implemented in an education setting, for example when working in the classroom or, remotely such as from home or in transit. Article 32 UK GDPR.
- *__Principle 7__ **("The Accountability Principle")** in detail;
  - Understand how to practically comply with the Accountability Principle which requires a Controller to not only comply with the data protection principles but to also be able to demonstrate that compliance;
  - Consideration of Accountability measures to demonstrate compliance which are both mandatory and optional such as data protection policies, designating a DPO, staff data protection training and carrying out Data Protection Impact Assessments (Articles 24 and 25 UK GDPR);
  - Data Protection Impact Assessments (DPIAs). When is a DPIA required? What must a DPIA contain? When must the ICO be consulted regarding a DPIA?
  - Understand the requirement under UK GDPR relating to staff data protection training and data protection policies;
  - Using the ICO's Accountability Framework to assess your organisation's accountability.

Part 4B: Data subjects' legal rights (Articles 12-17, 21-22 UK GDPR):

- Modalities common to all individual rights;
- ***Right to be informed*** (A.13 and A.14 UK GDPR);
  - Privacy Notices in educational establishments – the practicalities. What must be included and at what point in time must it be provided? Notices for younger children in age-appropriate language and in the spirit of the ICO's Children's Code;
  - Adopting the contemporary approach to privacy notices including use layering, icons and videos.

- ***Right of subject access*** (A.15 UK GDPR);
    - Controller's obligations; clarifying a Subject Access Request (SAR); time-limits and extending the time limit for compliance based on complexity;
    - SARs involving unstructured manual records;
    - SARs made on behalf of the data subject by a third party – considerations;
    - Refusing a SAR; refusing a SAR on the ground that it is "manifestly excessive" or "manifestly unfounded";
    - Refusing of a SAR in reliance on a legal exemption from the right of subject access. Exemptions covered include: Third party personal data exemption; exemption for exam scripts and exam marks; legal professional privilege exemption; exemption for SARS relating to "education data", "social work data" and "health data"; the significance of the status of "education workers"; the negotiations exemption; the management planning exemption; exemption relating to prevention and detection of crime; exemption relating to child abuse data; exemption relating to confidential references;
    - Effective management of SARs.
- ***Other individual legal rights*** *covered* include: Right to rectification; Right to erasure; Right to object to certain types of processing; Right to object to profiling and automated decision making;

- The Right of portability and the Right to restrict processing is ***not*** covered in the Foundation course and neither right is examinable.

Part 4C: Obligation to maintain a Record of Processing Activities (ROPA) (A. 30 UK GDPR):

- The Controller's obligation to maintain a ROPA, the exemptions from that obligation and the information which must be recorded;
- A Processor's obligation to maintain a ROPA is identified but not covered in detail and is not examinable.

Part 4D: Obligation to pay the annual Controller fee:

- The legal requirement to register with the ICO and pay the data protection fee (S. 137 DPA 2018); Calculating the data protection fee payable (Data Protection (Charges and Information) Regulations 2018);
- An overview of the exemptions;
- Penalties for non-payment.

Part 4E: Obligation in relation to international data transfers from the UK:

- A general and high - level review of an educational establishment's obligation, as a Controller. to ensure that any transfers of personal data from the UK comply with the UK GDPR rules relating to international transfers;
- An overview of the current legal framework relating to transfers from UK and transfers to the UK from the E.U.
- An understanding of the concept of a "restricted transfer", i.e., what amounts to a restricted transfer and what is not a restricted transfer. How to ensure that a restricted transfer is undertaken in compliance with UK GDPR;
- Overview of the mechanisms under UK GDPR to transfer personal data from UK to a third country including Adequacy Decisions; appropriate safeguards and derogations;
- Transfer Impact Assessments (TIA) – when should a TIA be executed?
- EU-US Data Privacy Framework of "DPF" and the UK data bridge to that framework which allows certified US companies to sign-up to be able to receive UK personal data through the framework;
- This topic is covered only at a general level in the Foundation course.

Part 4F: Obligation to designate a Data Protection Officer (DPO) (Article 37-39 UK GDPR (DPO) and non-statutory data protection lead roles:

- The course identifies which educational establishments must designate a DPO (the mandatory DPO), the role and tasks of a DPO appointed under statute and the Controller's obligations in respect of the DPO;
- Delegates will understand their obligations where they are *no*t subject to the statutory obligation to designate a DPO but choose to appoint one on a voluntary basis;
- The course also explores the appointment of non-statutory data protection leads which have no statutory status and whose role and tasks are not regulated by UK GDPR.

Part 4G: Obligations when sharing personal data with third parties:

- Exploration of an educational establishment's statutory obligations under UK GDPR when sharing/disclosing personal data with (i) an independent Controller and (ii) a Processor;
- Obligations under Article 26 when data sharing with a Joint Controller are identified in broad terms only and not covered in any detail or examinable in the Foundation course. They are covered and examined at the Advanced course and exam respectively;
- The requirements of Article 28 UK GDPR relating to contracts between your educational establishment (as a Controller) and a Processor; The practical application of Article 28 UK GDPR (contract requirements between Controllers and Processors) is also covered in Part B of the Foundation course in the context of contracts with EdTech service providers;

- Importance of the ICO's Data sharing Code of Practice, particularly in respect of sharing personal data relating to children.

Part 4H: Obligations in relation to personal data breaches:

- Delegates will understand what a personal data breach is and when the threshold for notifying a breach to the ICO, and impacted Data Subjects, respectively, is met (A. 33 UK GDPR);
- Delegates will understand the statutory internal logging requirements relating to breaches;
- The practical application of this aspect of the course is covered in Part B of the Foundation course where delegates are taught to recognise, manage and prevent breaches in an education setting.

Part 5: The role and powers of the ICO and enforcement:

- The role and powers of the ICO and aspects of the ICO's Regulatory Action Policy;
- ICO enforcement powers;
- Powers of prosecution for certain criminal offences relating to unlawful handling of personal data (unlawful obtaining under s. 170 DPA; re-identifying personal data under s. 171 DPA; alteration of personal data with intent to prevent disclosure under s. 173 DPA; penalties for breaches;
- Certain remedies available to a Data Subject for breaches.

Part 6: Horizon Scanning: Potential Changes to UK Data Protection Law through the Data Protection Digital Information Bill (No.2)

Section B: Application of UK Data Protection Law in an Education Setting

Part B of the training course is a practical application of data protection law in the context of specific data protection issues in an educational establishment using education specific examples. It also covers some practical skills for data protection leads in education settings to help achieve and maintain a culture of compliance.

Part 7: Using student images lawfully:

- Delegates will understand the appropriate lawful bases when processing student images for various different purposes and specific tripwires to consider when using student images;

- An exploration of the privacy issues raised by parents/carers taking photographs/video of other children at performances and sporting events and how to tackle it;
- The course will review recent enforcement decisions against educational establishments relating to misuse of student images.

Part 8: Data sharing with third parties;

Data sharing with processors including Education Technology (EdTech) service providers:

- Handling requests for disclosure of personal data from third parties who are independent Controllers including the Police, Local Authority/Children's Services (in the context of the exercise of child protection/safeguarding duties), and The Teaching Regulation Agency (TRA);
- Dealing with data sharing requests from the courts or solicitors in the context of private/family law legal proceedings;
- Data protection issues arising when sharing personal data with a Processor that is processing personal data on behalf of your educational establishment, such as a service provider;
- Data protection issues when sharing with EdTech providers; Contracts between educational establishments and Edtech providers;
- Delegates will learn, at a high level only, about the requirements of Article 8 UK GDPR and how to comply, when processing the personal data of a child under the age of 13 years, on the lawful basis of consent, in the context of an Internet Society Service (ISS);
- Age-Appropriate Design Code; Delegates will learn what it is, when it applies and to whom it applies.

Part 9: Using personal devices ("Use Your Own Device" UYOD) and remote working - data protection compliance:

- Delegates will understand that data protection obligations continue to apply even when personal data is being processed on devices that are not owned by the educational establishment ("UYOD") or when staff are working remotely;
- Delegates will learn about the specific data protection risks arising from UYOD and remote working and how to mitigate those risks;
- ICO's published guidance on UYOD and remote working.

Part 10: Recognising, handling, and preventing personal data breaches:

- Consequences of a breach; breach statistics by sector and type (not examinable);
- Data breach reporting obligations to the ICO and Data Subjects (A. 33 UK GDPR);

- Statutory duty to record details of breaches in an internal breach log regardless of whether the breach is reportable;
- Key tripwires in an educational environment and preventing breaches in the first place;
- Dealing with an internal data breach: the process.

Part 11: Understanding the Data Protection Compliance Implications of Using of Artificial Intelligence (AI) in an Educational Environment; an overview:

- Understanding what is meant by AI, generative AI and its typical applications in an educational environment including both the classroom and HR applications;
- AI considerations in the context of the data protection principle of lawfulness, fairness and transparency; legal bases, transparency, fairness and the right to object;
- Data protection and privacy considerations where AI is used for teaching and learning;
- Department for Education Policy Paper "Generative Artificial Intelligence (AI) in Education";
- AI considerations in the context of HR including recruitment and selection, CV screening, employee performance evaluation, and training;
- AI and the requirement for accountability;
- AI in the context of profiling and automated decision making (ADM) is considered at a high level only;
- The case for an AI Policy.

Part 12: Achieving and maintaining a culture of compliance in an educational establishment (not examinable)

APPENDIX 2. SAMPLE ASSESSMENT QUESTIONS

The Certified Data Protection Practitioner in Education/Foundation (CDPPE/F) examination lasts 90 minutes and contains 50 multi choice questions. Examples of the type of questions in the exam are found below. However, if you work in an educational establishment, are considering sitting the examination, and would like to receive more sample questions, please email: admin@mytenjin.com

The format of the CDPPE/F examination consists of 50 multiple-choice questions. Each question carries 1 mark. The first 40 questions are regular multiple-choice questions. The last 10 multiple-choice questions relate to TWO scenario-based questions; each scenario-based question has 5 multiple-choice questions.

Example of multiple-choice questions (There is only one correct answer.)

Q1. Which of the following is **NOT** an example of personal data?

a) A newspaper story about your head teacher.
b) CCTV images of specific pupils in the playground.
c) Xray images of your own broken leg.
d) A modern but controversial biography of Einstein.

Q2. What is **NOT** an example of special category personal data?

Recorded details that reveal the fact that a specific teacher …..

a) is bisexual.
b) has a criminal record.
c) is a super COVID spreader.
d) is a Quaker.

Q3. Which of the following is a personal data breach?

a) The college medical centre accidentally sending an email containing a student medical record to the wrong member of staff.
b) You sending a very personal email about yourself to the wrong friend.
c) Sending a data subject an email containing false statements that are damaging to the data subject's reputation (libel) about the data subject's behaviour at a staff meeting.
d) Leaving a printout of a sensitive email on top of a secure office printer in your office.

Q4. What is **NOT** an example of a processing operation?

a) Putting a manual filing system into a lorry prior to its relocation to a new office.
b) Printing a name and address sticker for a postal package.
c) Composing a private email to your partner.
d) Writing software to manipulate a database of personal data.

Q5. A multi academy trust receives a Subject Access Request (SAR) under Article 15 of UK GDPR from solicitors acting on behalf of a member of staff, for a copy of their personal data. The Trust considers the SAR to be complex because it involves Social Work Data, Health Data and there is a connected legal claim for discrimination against the Trust. By how long can the Trust extend the usual one calendar month deadline for compliance?

Which **one** of the following statements is correct?

a) A further three months.
b) A further two months.
c) A further one month.
d) By a reasonable period of time.

Example of scenario-based questions

There are 2 of these scenario-based questions in the exam, each comprising 5 multiple-choice questions (questions 40-50). Read the scenario and answer the multiple-choice questions that follow:

Scenario 1

A preliminary case conference by Zoom/Teams is called by Children's Services of a Local Authority to review a potential safeguarding/child protection allegation involving a nine-year-old pupil at your school, made against the new partner of one of their parents.

The attendees include a social worker from the local authority, the relevant class teacher from the pupil's school, and a GP from a local NHS practice.

Minutes summarising the views of the attendees and meeting outcomes were prepared by the social worker and emailed to all meeting attendees. The parents or police were not invited to this preliminary meeting and were not sent a copy of the Minutes.

End of scenario

Identify the correct answer to the following questions. Only **one** of the four statements is correct:

Q6. In data protection terms which **one** of the following statements is correct?

a) The teacher, social worker and GP are three independent controllers.
b) The teacher is a processor as he/she is providing processing services to the GP Practice and social worker when compiling the minutes.
c) The school is the only controller in the scenario.
d) The pupil, the teacher, the GP and social worker are all data subjects.

Q7. With respect to data subject rights which **one** of the following statements is correct?

a) The personal data collected at the meeting must amount to a breach of the Transparency Principle as no Privacy Notice has been given to the parents.
b) Each parent has the right to object to the processing of personal data collected at the meeting because the meeting was held in their absence.
c) Either parent can exercise the right of access to their own personal data, subject to the application of an exemption from the right of subject access.
d) The right to erasure is likely to succeed when applied to personal data comprising the professional opinions of the teacher, social worker or GP.

Q8. With respect to the Data Protection Principles, which **one** of the following statements is wrong?

a) Professional but erroneous opinions of the teacher, GP or social worker in the minutes are very likely to be consistent with the Accuracy Principle.
b) Concerns expressed in the minutes that a crime could have been committed are excessive or irrelevant because there was no police officer present at the meeting.
c) Taking and retaining minutes of the meeting help comply with the Accountability Principle.
d) In the minutes, it would be good security practice to identify the pupil by his/her initials or pupil identification number rather than by full name.

Q.9 Which **one** of the following statements about the minutes is correct?

a) If there are no child protection issues, the data protection principle that relates to transparency of processing requires the parents of the pupil to be immediately provided a copy of the minutes.
b) In the absence of the police attending the case conference, if the minutes are then disclosed to the police, the disclosure will amount to a breach of the lawful processing requirements of the first data protection principle.
c) Information disclosed in confidence by the pupil to their teacher, about the behaviour of one of their parents, can be exempt from the right of subject access by that parent.

d) If there are no child protection issues, the Storage Limitation Principle requires the minutes of the meeting and any related documentation to be deleted as soon as possible after the meeting.

Q.10 Where the parents of the pupil make a Subject Access Request (SAR) to the school for personal data relating to their child within the minutes, which **one** of the following statements is correct?

a) The school must provide a copy of the requested personal data relating to their child within one calendar month.
b) The school may be able to process the SAR if they are satisfied that the SAR is genuinely made on behalf of the pupil and in the pupil's best interests.
c) The school cannot disclose the child's personal data to the parents without the child's fully informed consent.
d) The school may only process the SAR on behalf of the parents subject to an Order of the court.

Scenario 2

You are a DPO in a fee-paying independent school in secondary education. Your Headteacher is about to contract with a company ("EduPredicter") that uses Artificial Intelligence (AI) to identify "highflyer" students and those needing additional support.

EduPredicter also processes the student personal data to further develop their software.

The AI algorithm measures student metrics by processing the following personal data: student identification details, exam results, Special Educational Needs (SEND), attendance, absence, ill-health and medical information, time keeping records, pastoral records (disciplinary sanctions or welfare issues), sporting attainments, browser history on school ipads etc., records of meal choices and library book borrowing, parents' occupations.

The AI model is capable of analysing the student's personal data to predict a student's exam performance trajectory, and limitations likely to be encountered by the student in their future career.

End of scenario

Identify the correct answer to the following questions. Only **one** of the four statements is correct:

Q.11 In data protection terms, which **one** of the following statements is correct?

a) In respect of all the students' personal data described in the scenario, the software provider is a Processor.
b) In respect of the students' personal data processed for AI software development, the software provider is an independent Controller.
c) In respect of the students' personal data processed for AI software development the school is a Controller.
d) The school and the software provider are Joint Controllers as they have a contract covering both purpose and manner of processing the student data.

Q.12 In data protection terms which **one** of the following statements is correct?

a) The most appropriate lawful basis for the school's processing of student personal data is that the processing is necessary for the purposes of fulfilling a contract that covers all aspects of delivering an education.
b) In order to ensure that the processing is fair and transparent, prior to any processing, the school will need to provide both students and parents/carers a Privacy Notice which explains what personal data is being processed, why, and with whom it is being shared.
c) If student personal data is processed in pseudonymised form there is no need for the school to identify a legal basis for the processing.
d) The most appropriate lawful basis for the school to process any health personal data relating to a student's accidental injury on the sport's field is that the processing requires the explicit consent of the student.

Q.13 Assuming the school is acting as a Controller and the software provider is acting as a Processor, which **one** of the following statements is **incorrect**?

a) The school has a statutory duty under the UK GDPR to carry out pre-contract due diligence checks of the software supplier to ensure that it is capable of providing sufficient guarantees to implement measures that will ensure compliance with the UK GDPR.
b) The processing of the personal data must be governed by a legally binding written contract between the school and the software provider.
c) The contract between the school and the software provider must stipulate that if the software provider experiences a personal data breach it must notify the ICO without delay and in any event within 72 hours.
d) The contract between the school and the software provider must stipulate that the software provider acting as Processor must only process the personal data on the documented instructions of the Controller.

Q.14 In data protection terms which **one** of the following statements is **correct**?

a) When a student leaves the school, EduPredicter can choose to either erase the student data or return it to the school, because it is no longer needed.
b) After a student leaves, EduPredicter can repurpose the student data to further develop its AI software, in pseudonymised format so that GDPR will not apply to its processing of the data.
c) If EduPredictor receives a Subject Access Request from a current student, it must ensure that it handles the request within the UK GDPR statutory timeframe and send the school a copy of its response.
d) If EduPredicter uses other sub Processors to help it deliver its services to the school, EduPredictor must have the school's written authorisation to appoint a sub-processor.

Q.15 EduPredicter experiences a brief cyber-attack affecting the personal data it is processing on behalf of the school. It recovers the situation and does not believe there is any risk to data subjects arising from the data breach. In data protection terms which **one** of the following statements is **CORRECT**?

a) As the data breach is unlikely to result in a risk to the rights and freedoms of any individual, there is no need for the school to record details of the data breach internally.

b) If, contrary to EduPredicter's view, the school is satisfied that the breach is likely to result in a risk to the rights and freedoms of individuals, then the breach has to be reported to the ICO.
c) If the breach is likely to result in a high risk to the rights and freedoms of individuals, the school is required to notify the individuals about the breach within 72hrs.
d) EduPredicter, as processor is not obliged to notify the school of the data breach because there is no risk to data subjects.