

Data protection and data security policy

Statement and purpose of policy

Path Examinations Ltd. is committed to ensuring that all personal information handled by us will be processed accordingly to legally compliant standards of data protection and data security.

The purpose of this policy is to help us achieve our data protection and data security aims by:

- a. notifying our candidates of the types of personal information that we may hold about them and what we do with that information
- b. ensuring candidates understand our rules and the legal standards for handling personal information relating to candidates and others.

Responsibility for data protection and data security

The Managing Director has overall responsibility for ensuring that all personal information is handled in compliance with the law and has appointed himself as Data Protection Officer with day-to-day responsibility for data processing and data security.

Personal information and activities covered by this policy

This policy covers personal information which:

- a. relates to a living individual who can be identified either from that information in isolation or by reading it together with other information we possess
- b. is stored electronically or on paper in a filing system
- c. in the form of statements of opinion as well as facts
- d. which relates to candidates (present, past or future) or to any other individual whose personal information we handle or control
- e. we obtain, hold or store, organise, disclose or transfer, amend, retrieve, use, handle, process, transport or destroy.

Personal information processed about candidates

We collect personal information about you which:

- a. you provide or we gather during the exam registration process
- b. is provided by third parties, such as learning centres and academies
- c. is in the public domain.

The types of personal information that we may collect, store and use about you include records relating to your:

- a. home address and contact details as well as contact details for your next of kin
- b. gender and date of birth
- c. marks and grades awarded in Path exams.

We will use information to administer your exam registration, your examination, notification of marks and grades, certification, and to deal with any problems or concerns you may have including:

- Equal Opportunities Monitoring: to conduct monitoring for equal opportunities purposes and to publish anonymised, aggregated information about the breakdown of Path candidates.

We confirm that for the purposes of the Data Protection Act 1998, Path Examinations Ltd. is a Data Controller of the personal information in connection with your registration. This means that we determine the purposes for which, and the manner in which, your personal information is processed. If you consider that any information held about you is inaccurate, then you should contact Path Examinations Ltd. and, if we agree that the information is inaccurate, then we will correct it. If we do not agree with the correction, then we will note your comments.

We will take reasonable steps to ensure that your personal information is kept secure, as described later in this policy and in general, we will not disclose your personal information to others outside the company. However, we may need to disclose personal information about candidates:

- a. for the administration of your examination
- b. to comply with our legal obligations or assist in a criminal investigation or to seek legal or professional advice, which may involve disclosure to our lawyers, accountants or auditors and to legal and regulatory authorities, such as HM Revenue and Customs
- c. to other parties which provide products or services to us.

By providing your personal information to us, you consent to the use of your personal information (including any sensitive personal data) in accordance with this policy.

Data protection principles

All staff, contractors, coordinators, consultants and international partners of Path Examinations Ltd. must comply with this policy and with the eight legal data protection principles which require that personal information is:

- a. processed fairly and lawfully. We must always have a lawful basis to process personal information. In most (but not all) cases, the person to whom the information relates (the Subject) must have given consent. The Subject must be told who controls the information (us), the purpose(s) for which we are processing the information and to whom it may be disclosed
- b. processed for limited purposes and in an appropriate way. Personal information must not be collected for one purpose and then used for another. If we want to change the way we use personal information, we must first tell the Subject
- c. adequate, relevant and not excessive for the purpose
- d. accurate. Regular checks must be made to correct or destroy inaccurate information
- e. not kept longer than necessary for the purpose. Information must be destroyed or deleted when we no longer need it. For guidance on how long particular information should be kept, contact the Managing Director
- f. processed in line with Subjects' rights. Subjects have a right to request access to their personal information, prevent their personal information being used for direct-marketing, request the correction of inaccurate data and to prevent their personal information being used in a way likely to cause them or another person damage or distress
- g. secure. See further information about data security below
- h. not transferred to people or organisations situated in countries without adequate protection.

Data security

Path Examinations Ltd. is committed to protecting personal information in our possession from being accessed, lost, deleted or damaged unlawfully or without proper authorisation through the use of data security measures.

Maintaining data security means making sure that:

- only people who are authorised to use the information can access it
- information is accurate and suitable for the purpose for which it is processed
- authorised persons can access information if they need it for authorised purposes. Personal information therefore should not be stored on individual computers but instead on our central system.

By law, we must use procedures and technology to secure personal information throughout the period we hold it, from obtaining to destroying the information. Personal information must not be transferred to any person to process (e.g. while performing services for us), unless that person has either agreed to comply with our data security procedures or we are satisfied with other adequate measures.

Security procedures include:

- physically securing information. Any desk containing confidential information must be kept locked. Computers should be locked with a password when they are left unattended and discretion should be used when viewing personal information on a monitor to ensure that it is not visible to others
- controlling access to premises. Staff, contractors, coordinators, consultants and international partners should report to security if they see any person they do not recognise in an entry-controlled area.

Telephone precautions: Particular care must be taken by staff, contractors, coordinators, consultants and international partners of Path Examinations Ltd. who deal with telephone enquiries, to avoid inappropriate disclosures. In particular:

- the identity of any telephone caller must be verified before any personal information is disclosed
- if the caller's identity cannot be verified satisfactorily, then they should be asked to put their query in writing
- to not allow callers to bully them into disclosing information and, in the event of any problems or uncertainty, contact the Managing Director.

Methods of disposal: Copies of personal information, whether on paper or on any physical storage device, must be physically destroyed when they are no longer needed. Paper documents should be shredded and CDs or memory sticks or similar must be rendered permanently unreadable.

Subject access request

By law, any Subject (including candidates) may make a formal request for information that we hold about them, provided that certain conditions are met. The request must be made in writing. In some circumstances, it may not be possible to release the information about the Subject to them, e.g. if it contains personal data about another person. Any member of staff, contractor, coordinator, consultant and international partner who receives a written request should forward it to the Managing Director immediately.

Review of this policy

Date: 15th January 2021

Review date: 15th January 2022