

Q-INTERACTIVE AND Q-GLOBAL SECURITY AND PRIVACY: ONLINE AND DIGITAL TESTING AND THE AUSTRALIAN PRIVACY PRINCIPLES (APP)

Pearson Australia takes data security and privacy seriously. Whilst we do everything required by our legal obligations, we also understand this is of importance to our customers and test-takers. Our Q-interactive and Q-global systems meet the Australian Privacy Principles (APP) standards for storing and processing personal information.

Pearson Australia offers products and services which are developed in collaboration with its global Clinical and Talent Assessment division. This allows Pearson Australia to offer an Australian focused product backed by Pearson's global expertise and knowledge.

All export of personal data collected via Q-interactive and Q-global only occurs with consent (which is why we are open about the Canada data storage in our documentation, including FAQ). Our privacy policies on our website explain in detail how Pearson is committed to keeping your data safe and protected.

Is Pearson's storage of personal data from Q-interactive and Q-global compliant with the Australian Privacy Act 1988 (Cth) and the Australian Privacy Principles (APP)?

Yes

Where will the test-taker data be stored?

Where Pearson Australia offers online testing products via Q-interactive and Q-global, all test-taker data will be stored on computer servers located in Canada. The primary servers are located in Montreal and Toronto. The back-up servers are located in the Central Canada region.

Why is the data not stored in Australia?

At this time, Pearson Australia has made a decision on operational grounds that it can best achieve the type and level of security which it feels is required by using the servers in Canada, in conjunction with the other global Clinical and Talent Assessment units within Pearson. Pearson has deployed global expertise in terms of data security which is justified by the volume of data in the Canadian servers.

Replicating that level of security (both physical and technological) would add significantly to the costs incurred by Pearson Australia customers.

Is Pearson allowed to store the data in Canada?

Yes. Pearson Australia follows the provisions set out in the Privacy Act 1988 (Cth) around export of personal identifiable information from Australia.

Pearson Australia remains fully responsible to its Australian customers and test-takers for the security of the data at all times.

Australian Privacy Principle 8.2 allows export to jurisdictions which provide "substantially similar" protection to Australian law.

Canadian law imposes much stricter requirements for storage and processing of personal data in comparison to Australian law, and, Pearson's export of personal data (with consent) from Australia to Canada is lawful.

Other jurisdictions such as the European Union also recognise Canada's personal data and privacy regime as being of sufficient rigour to allow personal data exports without any further legal requirements.

How will examine data be secured?

Examinee data on the system is protected through physical security, administrative safeguards and encryption. Examinee data is de-identified and stored on servers located in a secured data centre in Canada in a database that is encrypted with industry standard high-security encryption. When the data is transmitted, the data is encrypted using industry-standard Secure Socket Layer (SSL) technology.

The system uses a secured Oracle database which separates and segregates a customer's records so that they cannot be seen by other customers. This separation and segregation is confirmed through testing and external auditing.

Access to any customer account and the data housed within is protected by customer account password. Customers are responsible for safeguarding passwords, and to change your password periodically and whenever there is a concern about a possible compromise. There is also no requirement for an examinee's name to be submitted to Q-interactive or Q-global.

The Canadian servers and site is regularly tested and subjected to audits, both internal and external, to ensure it meets the stringent requirements of Canadian law and Pearson's own internal policies.

What happens if an unauthorised user attacks the data centre and tries to steal my data?

Personally identifiable information, including examinee data, is encrypted on the system. Encryption is utilised to prevent an unauthorised person from being able to see or use the data.

What examinee data can Pearson system support personnel see?

Pearson system support personnel do not have access to personally identifiable examinee data or access to, or control over, the encryption keys. The encryption keys are securely held and protected through physical and administrative safeguards.

Who else has access to personally identifiable data?

Pearson Australia does not grant access to any third parties to personally identifiable data which is not previously authorised by the customer. We do not allow anyone to use it for marketing purposes in any way.

As the servers are located in Canada, provisions in US law around the Health Information Portability and Accountability Act (HIPPA) which allow insurance

companies access to any data do not apply. Moreover, no access is required by this law, as insurance providers are only allowed access to US-originating personally identifiable data. Australian customers would fall outside this category.

Can Pearson use my data for research?

Personally identifiable data cannot be used by Pearson for research except with your express written permission and consent.

Account owners have the ability to proactively allow, or not, the use of de-identified data from their account to be used for research purposes. This option will be presented to the account owner when they log into their account. The choice of the account owner will apply to all users on the account and can be modified by the account owners at any time.

Who do I contact if I have a query or complaint?

If you feel your personally identifiable data has been used in a manner that is unauthorised or in breach of the Privacy Act's requirements, you can contact Pearson Australia at: privacy.officer@pearson.com.au, or write to the Privacy Officer, 707 Collins Street, Melbourne, VIC 3008, Australia.

You can also contact the Office of the Australian Information Commissioner (www.oaic.gov.au) to discuss your concerns.