AWS Hosting FAQs

Q-interactive and Q-global moving to the cloud.

What's happening?

The Q-global and Q-interactive are moving out of the current Centurylink brick-and-mortar data center and into the Amazon Web Services (AWS) cloud. The systems and data will remain in Canada.

When is this happening?

We currently anticipate that this will happen during the summer of 2018. The migration will happen over a weekend, and we will experience approximately 8 hours of down for both Q-global and Q-interactive.

What is AWS?

AWS Cloud Services is a secure cloud services platform, offering compute power, database storage, content delivery, and a variety of other services designed for scalability, resiliency, and security. More information about AWS's cloud computing can be found here: https://aws.amazon.com/what-is-cloud-computing/

Does this mean that we're now using the Cloud?

Yes. Amazon is one of the largest cloud providers in the world, with multiple service regions across the globe. https://aws.amazon.com/about-aws/global-infrastructure/

Why are we doing this?

Q-global and Q-interactive are moving to the cloud in support of Pearson's broader strategy for increasing security for client data, as well as the systems that host it, improving recoverability and resiliency, increasing scalability, and brings in additional layers of resiliency against cyberattacks, such as *distributed denial of service (DDoS)* attacks.

Why is it more secure than the current solution?

The migration to AWS Cloud services constitutes a significant step forward in our efforts to continue to improve our information security and data privacy controls profile. As the information privacy regulatory landscape continues to intensify, requiring higher levels of regulatory compliance and greater attention on the details behind ensuring individuals' personal information is protected, so must our own ability to meet these requirements evolve.

We selected AWS based on Pearson's success and experience with its cloud-based deployments and because Amazon's cloud infrastructure meets a multitude of industry standard security frameworks and regulatory standards. Amazon's AWS solutions are

GDPR-ready, for those clients who are subject to it. To name just a few of the other industry and regulatory certifications, here is a small sample:

- ISO 27001
- SOC 1, 2, and 3
- PCI DSS Level 1
- FedRAMP
- FERPA
- NIST

For a full list, please visit Amazon's *AWS Compliance Programs* web page.

What about encryption?

While it is certainly possible to encrypt data-at-rest and data-in-transit in a traditional brick-and-mortar data center, the ease of doing so, compared to the capabilities of the AWS Cloud Services environment, is much higher. Storage services and functions come with AES-256 encryption capability as a default feature, making it easier to maintain and enable.

The AWS Cloud environment facilitates the ability to enable AES-128 encryption over current versions of *transport layer security (TLS)* encryption technology while moving between components within the cloud-based network. This functionality is also available to us for encrypting the data when it is in-transit between our systems and you, the customer.

In short, we have a much-enhanced capability to provide the highest level of security and encryption to protect the confidential and personal information you entrust to us. This includes such measures as FIPS-compliant encryption and strong public/private secret keys and key management.

What about data isolation capability?

In the AWS Cloud environment, isolation is achieved through the use of something called a *virtual private cloud (VPC)*. It becomes a secure network, distinct and separate from the network where our desktop workstations and users on our internal network reside. This makes it much harder for virus infections to reach or impact our production network.

In the typical brick-and-mortar setting, a firewall is the single point of entry for the entire company network—user workstations, development and test environments, production systems, and data repositories. Since they are all on the same network, the risk of malware infection is greatly increased.

In AWS, the use of VPCs, allows us the ability to isolate the production network and restrict access at much more granular level through Amazon's *Identity and Access Management (IAM)* system. The AWS IAM manages access to each VPC separately, adding a layer of security not found outside of the cloud.

Are there other benefits?

Without a doubt, *yes*! Scalability! One of the challenges with any brick-and-mortar data center is the ability to scale resources to meet the demands on the services provided, which can result in degraded performance and system outages. With the increased ability to scale up quickly in response to changes in load and demand, our ability to ensure better and more consistent service levels dramatically increase. Through standardized server builds, called *Amazon Machine Images (AMI)*, we can automatically launch new instances of compute resources in a matter of minutes upon detecting a significant change in performance and load.

Will there still be a disaster recovery site separate to the primary data center?

The AWS Cloud Services lends itself toward an evolution in disaster recovery and business continuity through an architecture built for *disaster avoidance*. Amazon's global services make use of multiple *availability zones (AZ)*, which are separate data centers spread across a given geographic region. This allows us to deploy and replicate services across multiple AZs to ensure high availability of services and resiliency against outages and cyberattacks that might otherwise impact service performance. Should any individual instance of the service in a given AZ experience a failure, the other AZs in the architecture can take over its functions.

The AZs we will be using are all located in the AWS Canada region, which (currently) has two AZs.

What will this mean for customers?

Customers should not notice any change in their use of either Q-global or Q-interactive. They will enjoy a variety of benefits, including:

- Improved reliability, stability and performance
- Enhanced security
- Greater ability to meet regulatory compliance requirements

And during the migration, we will make every effort to ensure the disruption for customers is kept to a minimum, and that the downtime window is communicated to customers as early as possible to allow customers to plan around this time.

Is customer data still stored in Canada?

Yes. Customer data will still be stored in Canada. Client data is transferred over an encrypted connection and stored in an encrypted database within AWS Cloud Services AZs in Canada, the exact data center locations for which are not disclosed to the general public—or even to us as their customer.

Are Pearson cloud sites in other parts of the world, besides Canada?

At this point in time, Q-global and Q-interactive will only use the AWS regions in Canada. As other regions around the world become locations where Q-global and Q-interactive become hosting locations servicing customers, rest assured our attention to compliance and regulatory requirements will ensure data resides in the country of residence where such requirements exist. Canadian data will remain in Canada. If this were to ever change, appropriate notification and regulatory compliance reviews would precede any actual change.