Preparing for GDPR

How we are preparing for the General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) comes into force in May 25 2018. As part of our preparation for these new data processing requirements, we recognise that our customers and stakeholders will want to understand what arrangements we already have in place, and what we are planning to have in place by 25 May 2018.

We began working on our plans for GDPR in 2017, including our family companies Doublestruck, DRS and Teachit. With support from experts and technical specialists we're working towards being compliant with the GDPR by 25 May 2018.

Registration with the Information Commissioner's Office

We are registered with the Information Commissioner's Office (ICO) (Registration No PZ694888) under the requirements of the Data Protection Act (1998).

Our information management accreditation

We're ISO/IEC 27001 accredited, which is the international Standard that describes best practice for an information security management system (ISMS). Accredited certification to ISO 27001 demonstrates that an organisation is following international information security best practices. We've been certified since May 2006 and our next re-certification is taking place in June and July 2018.

Secure storage, erasure and destruction of personal data

All our customer data is stored at AQA datacentres, at carefully selected external datacentres and in the public cloud.

Where any infrastructure is hosted and managed outside AQA, we carefully check the security arrangements and make this part of the contract with the supplier. This includes a risk assessment that includes checking compliance with GDPR. We use this assessment to set the limits and conditions under which the supplier can process personal data on our behalf and it is part of the supplier's contract obligations.

When we need to share information externally, we make sure that the information is appropriate, accurate and is not shared where commercially sensitive or in breach of data protection legislation.

Our technical and organisational security to protect personal data

We have clear procedures to ensure the confidentiality, integrity, availability and resilience of our data processing systems and services. The introduction of the General Data Protection Regulations (GDPR) has meant we've increased our controls around the protection and use of personal data. We have regular internal and external audits to check and strengthen our data security controls.

Penetration tests and vulnerability assessments are scheduled frequently on our systems, both in the development phases and for existing services.

- Vulnerability assessments are regularly planned events to help in the identification of potential weaknesses in systems and services.
- Penetration tests proactively attack the systems to find weaknesses and assist in understanding how easy they are to exploit.

The security of our systems

All organisations are at risk of threats to their computer systems, whether the threats are software-based – such as viruses, worms, malware and spyware in downloads or even on websites – or come from direct human intervention through hacking. To protect AQA against this threat we are committed to keeping our systems up to date and as secure as possible and we take a layered defence in depth approach. This includes monitoring the physical security of our buildings and data centres through to password security, establishing good practice policies and procedures and the implementation of a consistent schedule of monitoring, patching vulnerability and penetration testing across the estate.

All of these controls and measures, together with a robust security awareness training programme, allow us to identify and address threats and vulnerabilities in a timely manner and keep our systems secure.

Protecting personal data

To operate our business, we need to collect and use personal data about students, staff and others. Personal data held by AQA is collected and managed in a responsible, secure manner, in compliance with the General Data Protection guidelines (GDPR). Guidance on data privacy and protection is covered in the AQA Data Privacy and Protection System, and supported by the Information Security Management System – a collective set of policies and procedures.

Access to personal data within AQA is restricted to authorised staff that need that access to do their job. All information has a defined owner responsible for accuracy, integrity, and security of the information. Data Owners are responsible for ensuring that all legal, regulatory, and policy requirements are met in relation to specific information assets. Data Owners are also responsible for ensuring appropriate training is in place for their departments.

We take seriously our obligation to staff training and awareness. Interactive security awareness training modules, GDPR awareness training, Anti-Phishing training and continuous testing are all part of the training platform for staff when they join AQA and throughout their time with the organisation. These are underpinned by awareness modules and procedures on social media behaviour.

New terms and conditions that include GDPR requirements

As part of our move to GDPR compliance we will be introducing new terms and conditions that all users of our systems will need to accept. We are also updating our privacy notice to address the requirements for GDPR compliance.

Policies and procedures for dealing with data breaches

We have clear policies and procedures that include what we'll do if there is a data breach. Our AQA Security Incident Reporting Policy establishes the process for reporting and managing all incidents, events, and weaknesses including the reporting and managing of personal data breaches as stipulated under the General Data Privacy Regulation (GDPR) breach notification. If a data breach happens, an escalation process will invoke the Data Breach Response and Notification Procedures, including raising the Data Breach Notification to the Supervisory Authority and Data Subjects if appropriate.

Review of data management procedures

All our policies and procedures contained in our Information Security Management System and the Data Privacy and Protection System are reviewed every 18 months by our Security and Risk team and other responsible people in the organisation. Once updated, they are passed to our Information Security Forum for approval and subsequently communicated to AQA staff on our intranet. The review and update of the policies is controlled and audited by both internal and external auditors.

Data that AQA holds on schools

We will hold different data on each school, depending on the services that you subscribe to and the choices that you have made about how you use them. Our data map is being updated in April 2018 and, once complete, will be available for you to read as part of our terms and conditions.

Data retention periods

Our data retention policy is being updated in April 2018 and, once updated, will be available for you to read as part of our terms and conditions.

Submitting a Data Subject Request

The process for submitting a subject access request remains the same until 25 May when GDPR comes into effect. Find out how to submit a request.

We are currently updating our Subject Access Request process and will provide information on how you can access this new service on 25 May.