Data Protection

Data you provide will be held securely and in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA 2018). Your personal details will not be disclosed to third parties.

Project Q is not responsible for deciding how information you enter into Project Q is processed; data is processed on behalf of your organisation. Use of Project Q will be on the understanding that your organisation is registered with the Information Commissioner's Office and are adhering to the Data Protection Act.

Privacy

Cookies

During normal use of www.projectq.co we collect and store anonymous statistical information to analyse how the website is used in order to improve the user experience.

The student and teacher portal of my.projectq.co uses cookies as part of the running of the system. The information stored in a cookie is minimal and is not used for any other purpose than maintain a session on my.projectq.co.

Personal data you submit

The personal data you enter into Project Q is not used, shared or accessed via Project Q or shared with any third party. Our technicians do not have direct access to the names, email addresses or passwords of Project Q. Following appropriate security checks and confirmation from the school coordinator we are able to reset a password for a users' account if we are provided with an email address. Your school is ultimately responsible for the data submitted to Project Q. At the end of your school/Project Q subscription (and you do not wish to renew) your data will be fully erased from our servers.

Third Parties

We will never disclose any personal information from Project Q to any third party. Any requests for support will be passed directly to the relevant contact within the company.

Web Beacons

Email we send through Project Q uses web beacons (small Project Q Logo image). The web beacon itself does not contain any personal data but simply allows us to monitor whether emails have been correctly received.

Security

Secure Communications

Once you have logged into Project Q at https://my.projectq.co all communication between your web browser and our server is encrypted using at least 128 bit encryption (SSL). Communication of data between the server and our office is also encrypted.

Password Security

We encourage strong password usage by implementing a mechanism for users registering with Project Q. We are unable to access passwords as these are stored using a 'one way' encryption method. Users can request a password reset which is sent to their registered email address.

Physical Security

Our dedicated servers are hosted in a secure data centre in Coventry, England. The data centre is protected by multi-layered physical security and all access into and out of the building is monitored by a visual human check and proximity access tags along with 24/7/365 video surveillance.

Staff Security

We have a small, dedicated team with very low staff turnover. All members of staff who require access to data are DBS checked.

Backups

Our servers are protected by a robust mirroring system. Regular backups are also performed routinely at the data centre. In addition to this, a comprehensive backup is transferred and stored securely at our office each evening. Our disaster recovery plan would ensure that a serious outage and failure at our data centre would ensure that the Project Q service would be fully running from 2 – 12 hours.

Monitoring

Our servers and services are monitored 24/7/365 by an array of complex external sources. Any failures to our servers and services are communicated directly to our senior ICT director to ensure of a timely response.

Data Breaches

Although our robust security measures and specialist networking services will ensure of secure data, our procedures require that any breach is disclosed immediately, and we will endeavour to comply with the Data Controller and Data Protection Authorities.