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 (ac3 solutions limited) is not responsible for deciding how information you enter into Project Q is processed; data is processed on behalf of your organisation. Each school/college remains the Data Controller. 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.

Please review our Data Protection Policy, Data Processing Activities and Data Breach Policy.

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 normal running of the system. The information stored in a cookie is minimal and is not used for any other purpose than to maintain an active 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. Following appropriate security checks and confirmation from the school coordinator we are able to view data to help resolve issues such as a password reset or specific query. 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 erased from our production servers and removed from system backups at the end of their cycle.

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.

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 SHA-2 (384 bits) cryptography. Data is also encrypted at rest and further encrypted during our backup cycles.

PASSWORD SECURITY

We encourage strong password usage by implementing a mechanism for users registering with Project Q or users make use of the Microsoft Single Sign On option. 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 private cloud in London, 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.

Overview

STAFF SECURITY

Project Q is supported by a small, dedicated team. All members of staff who require access to data are validated through Disclosure and Barring Service.

BACKUPS

Our servers are protected by a robust mirroring system into a secondary data centre. Regular backups are performed routinely at the data centre. In addition, a disaster recovery backup is transferred and stored securely at our offices. Our disaster recovery plan would ensure that a serious outage and failure at our data centre could 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 external monitoring services. Failures or concerns to the service are communicated directly to our ICT team for speed resolution.

DATA BREACHES

We take data security seriously and have many measures and specialist networking services and monitoring systems to help keep data secure. Data breaches are to be disclosed to clients and we will endeavour to comply with the Data Controller and Data Protection Authorities.

This document was approved by A Cree, Director of Project Q (trading as ac3 solutions limited) on 10/08/2022 and is issued on a version controlled basis.

Signature: Date:10/08/22

Change History Record

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	A Cree	20.03.2019
2	Update to documents	A Cree	10.08.2022