NLTS P105 New Links Training Solutions IT Systems Usage & Security

NTLS uses the following products to communicate with learners and to process QQI certification events.

Administrate, QQI QBS, Microsoft Office Applications

Data Processor:Jim Tumulty

USER SUBSCRIPTIONS for all applications

- **NLTS** undertakes not to allow any User Subscription to be used by more than one individual Authorised User unless it has been reassigned to another individual Authorised User, in which case the prior Authorised User shall no longer have any right to access or use the Services and/or Documentation.
- **Users** access to information and applications will be controlled by the Data Controller
- **Users** will not knowingly access, store, distribute or transmit any Viruses (having taken all reasonable endeavours not to do so), or any material while using the Services that: (a) is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing, or racially or ethnically offensive; (b) depicts sexually explicit images; (c) is discriminatory based on race, gender, colour, religious belief, sexual orientation, disability; or(d) is or facilitates otherwise illegal activity and/or causes harm to any person or property; and NLTS has the right, without affecting NLTS's other rights, to disable access to any material that breaches the above.
- **NLTS and individual users,** shall use all reasonable endeavours to prevent any unauthorised access to applications and/or information.
- **Authorised Users** will ensure that User Names and Password assigned to all them are maintained and not shared with any third party.
- **Authorised Users** will use the applications and information in accordance with GDPR and company guidelines.
- **NTLS** will only record and use personal information in line with our GDPR policy. NLTS will not store PPSN or Date of Birth details for any learners on our Administrate System or within the Office 365 system. NLTS will need to use PPSN and Date of Birth information to process learners for certification. **(See S10.12 for more information)**
- **NLTS** uses an automated schedule to maintaining user passwords in Administrate and in Office 365. NLTS complies with QQI requirements in maintaining access to the QBS system which uses Microsoft verification software to gain access to the system
- **Transfer of information/documents:** the transfer of information and/or documents must be made under strict supervision and must be approved by the data controller. Transfer of approved (non-sensitive) e.g. course handouts/administration documents may be made through the share drive facility – see (NLTS P013). **The use of any form of transfer using compact discs, cloud technology, external hard drive, email or USB is wholly prohibited** and use of any prohibited data transfer mechanism will be viewed as a serious breach of the company's data protection policies and appropriate action will be taken.

Section 8F

Procedural Document/s:

NLTS P013 – adding documents to the share drive (public use)

Administrate – Trust Statement

Delivered from the World's Leading Technology Infrastructure

Our primary services are delivered via Amazon Web Services, the world's leading provider of technical infrastructure. More than a million customers in 190 countries, comprising over 2,000 government agencies, 5,000 educational institutions, and 17,500 nonprofits trust AWS every day with their operations, data, and infrastructure. AWS operates more than 10x the infrastructure of the next 14 hosting providers combined and is growing at a rapid rate. At this time, all of our infrastructure operates from within the Amazon EU Region (Ireland), and all data resides within the Amazon EU Region (Ireland).

High Availability and Redundancy

We operate a fully redundant mirror infrastructure in a separate AWS availability zone to which we can failover if necessary. The second AWS availability zone is geographically separate and receives a copy of transactions and data operations performed on our primary cluster in "real time". In the unlikely event of a total failure at our primary provider, we can transition operations to the secondary location within minutes.

Data Center Security

Our providers have an impressive security track record for safeguarding your data and operations. Our providers meet or exceed the following standards:

- SSAE16
- ISO 27001
- ISO 27002
- PCI Security Standards
- Privacy Shield Certified
- HIPAA Compliant (have signed a Business Associates Agreement with Administrate)

Backups and Disaster Recovery

All critical systems are backed up nightly in addition to our mirror system. All customer data is backed up nightly in addition to being replicated in "real time" to our mirror system. Backups are tested weekly. We have the ability to take additional "snapshots" of a system before making changes so that we can revert in the event of an unexpected outcome. Backups are taken nightly, encrypted, and securely transmitted and stored within Amazon S3 which provides for the data to be stored on no less than three physically independent devices for durability. Backups are customer specific, and data is not commingled.

GDPR Compliance

Administrate is GDPR compliant. Our agreements with our customers contain specific language identifying how we process and control data on your behalf. In summary, Administrate clients are the nominated Data Controller, and Administrate is the nominated Data Processor. We maintain a list of the Subprocessors we use on this page.

Administrate is ISO 27001:2013 Certified

Administrate has achieved ISO 27001:2013 certification. The certification and audit were performed by Coalfire, a cybersecurity audit firm with more than 16 years of experience and more than 1,400 government and commercial clients.

- View our certificate here.
- View the auditor's letter here.

Privacy Shield

The US subsidiary of Administrate has been certified for the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks. These were designed by the U.S. Department of Commerce and the European Commission and Swiss Administration to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce. You can find Administrate's certification record here.

Service Monitoring and Reporting

We have several different levels of application monitoring to ensure that services are being rendered according to acceptable performance standards.

- We provide a public operational service status page which documents our historical uptimes and provides information in the event of a service disruption.
- Uptime monitoring by a third-party (Pingdom) which notifies us when external services slow down or fail.
- Internal application instrumentation on server loads and performance, in case resources are consumed at unusual rates.
- We provide the status of unusual or degraded operations via our operations Twitter account: @Adm1nistrateOPS

Application and Data Security: A Top Priority

We employ many different layers of security to keep your data safe. These security policies and processes follow industry best practices whenever possible and are periodically reviewed for conformance and compliance.

- All authentication and data transfer is fully encrypted and conducted via TLS (the successor to SSL).

Section 8F

- We employ firewall protections that prevent unauthorised users from attempting to connect to us.
- We have separate privileges for customer data and application access, and customer data is not commingled.
- We employ an industry-leading third-party security scanning service to audit our externally-facing infrastructure to determine any possible security threats daily.