

NISQ D21 Third Party Policy

a) This Policy outlines standards involved in working with third parties, including NISQ Approved Centres, Centre Staff, consultants, all NISQ Staff, agencies and suppliers, as well as the standards expected of them.

b) Third Parties **MUST** make all reasonable efforts and exercise due diligence to ensure the ongoing compliance of NISQ Policies, Guidelines and use of their administration system including the NISQ eLearners Pathway.

1.NISQ and Third Parties

NISQ will deliver effective and proportionate monitoring. Means of evidencing reasonable efforts to ensure effective ongoing compliance may include (but are not limited to):

* ensuring the values of NISQ are reflected in the Third Parties delivering their Qualifications,
* establishing a named individual with lead responsibility for monitoring external compliance; NISQ External Centre Verifier
* developing clear reporting requirements with the third-party and regularly reviewing progress against pre-agreed performance, quality assurance and compliance targets; Visitations NISQ 10v
* defining how monitoring will be carried out, including establishing an appropriate frequency for monitoring based on an assessment of the risk posed by the third-party activity;
* approving and regularly reviewing third party compliance with teaching, training, including frequently observing the delivery of this training onsite;
* authorising content and materials for teaching and training;
* regularly conducting (and documenting the results of) monitoring, NISQ Approved Centre visits and/or the third party;
* setting out a clear policy for handling complaints and feedback, including the time frames, procedure for escalating and raising internally, and the transfer of information between NISQ and the third- party; NISQ D7 Complaints Policy
* setting out a clear internal procedure for members of staff to report any concerns they may have regarding the Third Party. NISQ D10 Whistle Blowing Policy
* agreeing an action plan with the third-party to address any concerns, where these are identified, through the NISQ Approval Panel
* Put in place a signed agreement outlining the use or representation of NISQ Qualifications – NISQ 01 NISQ Centre Director. Head of Organisation Commitment

“The Centre will not through advertising or any other activity bring the name of NISQ in to disrepute/damage reputation. Or present a Qualification as being Regulated when it is not, misrepresent the NISQ Qualifications in any way that would be considered misleading for learners or users of Qualifications. This is a serious event and will incur a sanction or removal of the NISQ Approval Status.”

2.Third Parties

Must not mis-represent NISQ or NISQ Qualifications, either through a person connected to the third party or in a statement, including advertising and comments on any internet blog or through social media.

This includes but not limited to;

* Misrepresenting the relationship between the third party and NISQ,
* Endorsement of any teaching and training methodology as being endorsed by NISQ when it does not,
* Advertising a Qualification as being an NISQ Regulated Qualification when it is not,
* Endorsing a Resource as being endorsed by NISQ when it is not,
* Using the NISQ Logo in a way that has not been permitted or changing the way the NISQ Logo looks in any way,
* Advertise themselves as being a NISQ Approved Centre before being Approved by NISQ,
* Advertise being able to deliver a specific NISQ Regulated Qualifications when it has not been approved to,

3.Sanctions

NISQ D18 Sanctions Policy

Sanctions are actions typically taken to influence conduct. If the assessments of a qualification or the associated quality assurance procedures are compromised and a breach of an agreement, policy or regulation has occurred, NISQ will apply sanctions. The primary aims of applying sanctions are to:

* Protect and minimise the risk to the integrity of NISQ Regulated Qualifications and/or the quality assurance process.
* Protect all aspects of NISQ awarding of results and certificates.
* Allow NISQ to investigate suspected maladministration/malpractice while maintaining the integrity of the NISQ Regulated Qualification(s) involved.
* Protect the interest of Learners.
* Protect public confidence in the NISQ Regulated qualifications.

4.Standards and Third-Party Security

NISQ has created a set of exacting standards that should apply to third party suppliers; the most stringent of those standards need to be applied to those third-party suppliers who have access to information systems, data or the NISQ network. NISQ needs to be assured that the information is as secure as possible, and access and/or processing is only available to third parties who meet the NISQ standard. The following levels can be used as a guide to the required standards for suppliers before entering into contractual agreements:

|  |  |  |
| --- | --- | --- |
| LEVEL  | STANDARD  | GUIDANCE  |
| **1** – considered **Significant Risk**, Sanctions and/or suspension or Loss of Approved Status |  **ESSENTIAL** – NISQ Approved Centres i. Data Controller registration with ICO (unless exemption identified) ii. Compliance with NISQ Data Protection Policy NISQ D17iii. Data processing clauses (where appropriate- NISQ eLearners Pathway NISQ GL27iv. Enhanced Security Clearance Required | * Definite access to NISQ Data and/or network
* Personal identifiable information and/or business critical information
* Pseudonymised information on a large scale
* Safeguards need to be applied stringently to maintain security and prevent data loss
 |
| **2** – considered M**oderate Risk**, Sanctions and/or suspension or Loss of Approved Status | **Potential –**Third Parties - i. Data Controller registration with ICO (unless exemption identified) ii. Compliance with NISQ Data Protection Policy NISQ D17iii. Data processing clauses (where appropriate) iv. Enhanced Security Clearance Required  | * Potential access to network and/or data,
* Levels of potential access need to be assessed and the scope of the contract may not be fully understood.
* Personal identifiable and/or business critical data
* Pseudonymised data depending on scope and quantity

 NISQ Qualification Division will be able to assist in understanding the standards that will be required, usually all requirements will be valid as safeguarding NISQ network and data is essential and the ability to access poses a risk that requires mitigation.  |
| **3** – Considered **Minor Risk**Loss of contract with NISQ | **ONE REQUIRED** i. Non-disclosure clauses in contract or ii. Confidentiality agreementiii. Security Clearance Required | * Incidental access (e.g. window cleaning, maintenance)
* Access to pseudonymised / anonymised data
* On site presence / no direct access to data / network
 |
| **4.** considered **No Risk** | NO Compliance Standards Requirements | No access will occur; therefore, compliance is not required |

5 Compliance Explained

Data Controller Registration

 The Information Commissioners Office (ICO) hold a register of Data Controllers; the Data Protection Act, 1998 s1 details the following definitions:

* “data controller” means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;
* “data processor”, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;
* “data subject” means an individual who is the subject of personal data;
* “personal data” means data which relate to a living individual who can be identified

The personal data could include learner, staff and/or client information, a third party should look at their operations as a business and control over information to determine which category they fall into. If they are not registered but data controller for information this is illegal under the Act.

6 The ICO count the following as legitimate exemptions:

Most organisations that process personal data must notify the ICO of certain details about that processing. However, the Act provides exemptions from notification for organisations that process personal data only for:

* staff administration (including payroll);
* advertising, marketing and public relations (in connection with their own business activity); and
* accounts and records;
* some not-for-profit organisations;
* organisations that process personal data only for maintaining a public register;
* organisations that do not process personal information on computer.

Please note the difference between a Data Controller and Data Processor needs to be carefully considered and if there is any control over the processing purposes of the information the third party must be registered.

7 Compliance with NISQ Collecting and Protecting Information Policy NISQ D17

Refer to NISQ D17 available from [www.nisq.uk](http://www.nisq.uk) gives a level of compliance for Information Governance and Security practices for NISQ Approved Centres and applies to other third parties.