Acceptable Use Policy
Network Quarterly Data Collection (NQDC) application

1. About this policy

1.1. This Policy relates to the use of the Network Quarterly Data Collection (NQDC) application, hereafter referred to as ***the application***.

1.2. The purpose of the application is to enable the Health Innovation Network (HIN) to meet its reporting obligations to commissioners under the terms of the Master License Agreement, hereafter referred to as ***the business need***.

1.3. The application has been set up and is maintained by the HIN Informatics team at Health Innovation East, hereafter referred to as ***the Team***.

1.4. This Policy is written and maintained by the Team.

1.5. It applies to all users of the application provided with access privileges through a user account.

2. Accounts and passwords

2.1. User accounts are set up and managed by the Team. Access privileges will be granted to meet the business need in accordance with requests made by the Metric Lead in the corresponding HIN.

2.2. User accounts will be withdrawn when no longer required to meet the business need.

2.3. User accounts may be withdrawn in the event of a security incident or inappropriate use.

2.4. Users must keep their passwords confidential.

2.5. Users must only log into the application using their own username and password.

2.6. Users must not allow anyone else to log on using their username and password.

2.7. The Team must be notified immediately a user no longer requires access to the application.

3. Data security and confidentiality

3.1. Data held within and extracted from the application is confidential to the Health Innovation Network (HIN) to which it relates. It will be available to the HIN Central team and, subject to appropriate Confidential Information Data Sharing Agreements, may be shared with other HINs and commissioning bodies.

3.2. Users must comply at all times with the principles of the UK GDPR and have successfully completed appropriate information governance training.

3.3. Users are responsible for ensuring the security of confidential data and information.

3.4. Users must ensure that people without authorisation or legitimate purpose do not view or access data held by the application.

3.5. Users should ensure the security of confidential information on their devices and must not store any confidential information on their devices if using their own devices to access the application.

3.6. Metric Leads must be satisfied that all reasonable precautions are being taken by account holders in their HIN to maintain confidentiality of material in accordance with these Policy requirements.

3.7. If a user discovers or suspects there has been a data breach or an information security incident such as hacking or unauthorised accesses involving the application, they must report it to the Team within 24 hours.

3.8. In response to an information security incident, it may be necessary for the Team to shut down or block access to the application. Given the time sensitivity of managing such an incident, this may be done without previous warning.

3.9. Users are required to comply with any instructions and security measures implemented by the Team and to co-operate with any investigation into suspected data or information security incidents.

4. Appropriate use

4.1. The application and data within it may only be used in the course of activities to meet the business need.

4.2. Users must not engage in illegal activities (e.g. unauthorised access, data theft).

4.3. Users must not use resources for unauthorised activities, including commercial activities.

4.4. Users should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of their duties).

4.5. Users must not attempt to circumvent any security or authentication measures, including hacking our services.

4.6. Users must not attempt to access data or accounts for which they do not have authorisation.

4.7. The application and data within it must not be used for any commercial purposes, unless defined within the business need.

5. Breach of this Policy

5.1. Breach of this Policy may lead to the Team revoking access privileges to the application.

5.2. It may also result in disciplinary action up to and including dismissal or, in the case of a contractor, consultant, casual or agency worker, the termination of the engagement.

5.3. Users are required to co-operate with any investigation into suspected Policy breach.

Contact the HIN Informatics team
hininformatics@healthinnovationeast.co.uk

Review of this document: annually by the HIN Informatics team

Next review date: July 2025

Version	Amended content	Author	Date
AU Policy v1	New release	HIN Informatics team	May 2025