**City & Hackney CCG – Primary Care WIFI Policy**

1. **Introduction**

A free, public WIFI service was implemented in City and Hackney practices in 2017/18. Networks are available to staff and visitors to enable them to access the internet, send and receive emails, and download and access medical applications.

The service was commissioned by the CCG following a directive from NHS Digital. On the CCG’s behalf, NEL CSU initially carried out a mini-procurement and subsequently managed the implementation by the service provider Egton. Practices should familiarize themselves with this document and the Terms and Conditions in Appendix 2. Use of the service constitutes agreement to the Terms and Conditions.

# Purpose

The purpose of this policy is to ensure:-

* + There is an appropriate security framework in place for the provision of a public WIFI service;
  + There is suitable access and usage controls in place in line with NHS guidance and legislation;
  + Due attention is paid to the GP Practice/CCG’s legal obligations or to patient safety and confidentiality.

# Scope

The policy covers:-

* + All City & Hackney CCG GP Practice Sites and applies to any individual that may access the public WIFI service in any capacity at a GP Practice site including patients, members of the public, visitors, employees, students, volunteers and third party contractors etc.
  + Categories of websites permitted and blocked by the public WIFI service.

# Duties and Responsibilities

NHS Digital guidelines state that GP Practices are responsible for the following tasks. Each practice must assign a job role to the task. The CCG commissioned Egton service desk are responsible for user account administration.

|  |  |
| --- | --- |
| **Job Role** |  |
| Practice to complete | *The Practice will take full responsibility for the effective implementation of this Policy if it decides to provide practice staff and clinicians with access to the NHS WIFI service.* |
| Practice to complete | *The Practice will ensure that staff are adequately briefed on all information risks associated with free public WIFI access.* |
| *Egton Service Desk* | *User Account Administration – New users, Users deletion and user modification.*  *Requests will only be managed where a user has completed the WIFI user registration form included in the appendices of this policy.* |

1. W**IFI Availability**

Users are advised that NHS WIFI access is available across all sites but maybe subject to capacity restraints and WIFI signal availability. At busy times, the speed of the WIFI connection may be reduced or lost due to the number of users using the facility. If this occurs, users will have to try to access the WIFI service at a later time.

1. **WIFI Networks at each Practice**

There are four WIFI networks available at each site (this may vary at sites where two or more practices are co-located). They are identified by a Service Set Identifier (SSID). Two of these networks are served by the practices secure HSCN connection and two by a stand-alone public ADSL broadband connection. The networks provided are described in the following table.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SSID** | **Connectivity** | **Credentials Required** | **Access Provided** | **Devices that can use this network** |
| NHS WIFI | Public ADSL | No | Unsecured Internet Access for Patients and the general public. Bandwidth is limited. | Patient’s personal devices |
| Guest (CDB Number)  *e.g Guest 1234* | Public ADSL | Yes. Username and Password. A generic username and password provided for each site that allow concurrent access to the internet. | Provide internet access with no bandwidth restrictions. | Staff member, visiting GP and Health Professional’s personal devices.  Tele-derm iPhone. |
| NHS Secure (CDB Number)  *e.g NHS Secure 1234* | HSCN | Yes. Username and Password | Provides access to Practice LAN (if permissions granted in Active Directory), Clinical application and internet access. | NEL CSU/Egton managed devices only. |
| NHS City & Hackney CCG | HSCN | Yes. Username and Password (these are the same as the credentials used to access the Secure network) | Provides access to Clinical system from any GP site for GP’s and practice staff. Also internet access. It does not provide access to a practice Local Area Network (LAN) | NEL CSU/Egton managed devices only. |

# Accessing the WIFI Service

Practice Staff and Patients are free to use their personal devices to connect to the public services but must act considerately. The GP Practice’s do not allow any recording of photos, audio recording, videoing or the streaming of videos as this would severely affect a patient’s right to confidentiality and privacy.

The WIFI networks are accessed by selecting the appropriate SSID and entering the appropriate credentials.

Any individual who takes up the free NHS WIFI service at a GP Practice does so at their own risk. There is no staff support available for the administration of the service. Practice Staff are employed to provide essential clinical care to patients and not IT technical support where patients may experience trouble connecting to the WIFI. Any issues accessing the WIFI Network should be reported to the Practice. The Practice will report all technical issues to the EGTON helpdesk as described in the support document in the appendices of this policy.

Any devices considered to be network intrusive that potentially could interrupt the GP Practice/ CCG’s network services, or change the Network topology in any way are strictly prohibited.

# WIFI Terms and Conditions

In supplying a free public WIFI service all users are expected to comply with the Supplier’s fair usage Terms and Conditions. (Please see Appendices). Users are asked to read the terms and conditions of the agreement.

The standard WIFI offering provides a filtered service and strictly prohibits access to a number of category sites. Sites blocked include, but not limited to:-

* + Pornographic material;
  + Gambling;
  + Indecent images of adults and children;
  + Cyber bullying;
  + Terrorism;
  + Abused Drugs;
  + Alcohol and Tobacco;
  + Bot Nets
  + Confirmed SPAM Sources;
  + Cult and Occult;
  + Dating;
  + Games;
  + Gross;
  + Hacking;
  + Hate and Racism;
  + Illegal;
  + Keyloggers and Monitoring;
  + Malware Sites;
  + Open HTTP Proxies
  + Pay to Surf;
  + Peer to Peer;
  + Phishing and Other Frauds;
  + Proxy Avoid and anonymous;
  + Sex Education;
  + Shareware and Freeware;
  + SAM URL’s
  + Spyware and ?Adware;
  + Swimware and Intimate Apparel
  + Violence;
  + Unconfirmed SPAM sources;
  + Weapons

This list is not exhaustive.

Users must not access the above sites or use the facility to post, transmit, upload or download information that:-

* + May be considered unlawful, immoral or improper;
  + May cause unwarranted harm to any individual or employee;
  + Bring the Trust into disrepute or bring about legal proceedings.

Users will experience an access denied page where access is blocked.

# WIFI Risks

There are many risks associated with using the internet that users should be mindful of:

* Children filters are not in place to prevent inappropriate access to web content.
* A standard fair usage policy applies to all users.
* Patients are advised that the GP Practice/CCG’s network is open (i.e. not encrypted) and therefore cannot guarantee the security of some online networks for instance online banking, purchasing and personal communication such as Yahoo and Hotmail etc. Staff and patients are advised to refrain from these types of activities. The Practice/CCG is not responsible for the loss, misuse or theft of any information, passwords or other data transmitted via our network. The GP Practice/CCG can therefore not guarantee the confidentiality, integrity and security of any user’s information on the Trust network.
* Users must not post any confidential or personal data about the GP Practice/CCG’s, its staff and patients. Such postings will be treated as a serious breach of confidentiality and will invoke an investigation under *“The Reporting of a Serious Information Governance SIRI Policy (IG11)”.* Remember, whatever data you post may remain available in the public domain for decades afterwards. Users are asked to consider what they post before they do it.

# WIFI Monitoring

All users are advised that blocked access to inappropriate content is monitored. This is done in line with the Computer Misuse Act 1990 and the Lawful Business Practice (Interception of Communications) Regulations 2000.

Activity monitoring is provided to NHS digital as part of utilisation monitoring

# Violation and Non-Compliance

Any violation of this Policy will constitute as unacceptable behaviour and may result in the loss, suspension or termination of the service as set out in the fair usage Terms and Conditions in the appendices.

# Incident Reporting

There is now a requirement for all serious breaches of confidentiality or near misses to be reported via the DSPTK Incident Reporting System to the Department of Health and the Information Commissioner’s Office.

All users are advised that they are fully liable for their own actions and may be subject to criminal prosecution by the regulatory bodies or the affected data subjects where there has been a violation of this Policy.

# Dissemination

This Policy will be published and made available to all staff members along with other practice documentation

# Review

This Policy will be reviewed annually by the CCG to monitor alignment with national guidance / legislation. The practice manager and/or IG lead at individual practices may also wish to review to ensure alignment with practice data security policies. In the event that a practice reviews and wishes to make changes to the Policy, they should contact the CCG with the proposed change so it can be incorporated.

1. **Appendices**

|  |  |
| --- | --- |
| NHS WIFI Support Detail – C&H CCG |  |
| Egton WIFI User Registration Form |  |
| Egton WIFI Terms & Conditions |  |