NHS
Derby and Derbyshire
Clinical Commissioning Group

Away From My Desk

Process & Responsibilities

Contents

NHS
Derby and Derbyshire
Clinical Commissioning Group

Process for requesting Away From My Desk

Please consult the Feature Comparison tab in the NECS CSU Implementation spreadsheet which accompanies this document to ensure that Away From My Dest provides the functionality that you require for your GP Practice.

1. GP Practice will need to fully complete the NECS CSU Implementation spreadsheet attached to the email accompanying this document, including the following information:
    a. Surgery Name
    b. ODS Code
    c. Forename
    d. Surname
    e. Email Address
    f. Job Role
    g. Asset Number of the NECS device you wish to connect to in the practice
    h. Machine friendly name (e.g. NECS123456 Consulting Room 1, etc)

    Please ensure that person submitting the forms has read and agrees to the terms and conditions contained in Appendix A of this document and distributes the document in Appendix B to the end user to notify them of their obligations when using the software.

2. Once the spreadsheet is completed, please send this to derby@awayfrommydesk.com

3. Where the GP Practice has been migrated to the GPN domain, the user will be able to log onto their device within the GP Practice and download the software from the NECS Self Service Portal. If the user is unable to do this, another member of the Practice staff can install this on their behalf.

4. Where the GP Practice is still on the GP domain, the Away From My Desk team will notify the NECS Support Desk of the asset numbers of the devices requiring the software and this will be installed remotely, but requires the Practice PC to be turned on to do this.

5. Once the order has been processed, Away From My Desk will email each user individually with their details

    Please note that the user account cannot be activated without the software first being installed onto the device in the GP Practice

Appendix A – Practice Responsibilities

- The Practice is responsible for ensuring it satisfies all of the pre-requisites for approval to use the AFMD Biometric Edition remote access solution – see Appendix 1.
- The Practice is ultimately responsible for ensuring that remote access by staff is managed securely.
- The Practice is responsible for carrying out Home Risk Assessment Surveys for each staff member requesting the remote access solution.
- The Practice is responsible for ensuring the member of staff using the remote access solution has been trained in its use and is aware of their information governance and security responsibilities.
- The Practice is responsible for keeping records of all approved remote access users and these can be requested by the NECS for audit purposes.
- Practices that purchase AFMD Biometric Edition must agree and sign these Terms and Conditions.
- It is the responsibility of the practice to ensure they read and comply with these Terms & Conditions.
- It is the responsibility of the practice to replace lost or stolen AFMD Biometric Edition hardware and to immediately inform Away from My Desk, who is responsible for disabling the appropriate device and connection.
- The practice is responsible for keeping records of lost or stolen AFMD Biometric Edition hardware.
- The practice will be accountable for any misuse by staff from, or representing the practice and any costs resulting from this misuse will be borne by the practice.

Please note that by returning the spreadsheet the Practice Manager / GP Practice ICT Lead is confirming acceptance of the above terms and conditions.

Appendix B – End User Responsibilities

The remote solution must **only** be used in the following ways:

1) From the user's home - **provided** a current up to date manufacturer-supported operating system and appropriate, fully functional anti-virus, anti-spyware and firewall software products are installed on the remote PC/laptop. This **excludes** free software product versions such as, but not limited to, AVG, Avast, Avira, etc. as these are cut down versions, which do not have the full functionality of the commercial version.
2) From a laptop that has been encrypted by NECS.

NB: Users must not use the remote access solution from any public areas such as internet cafes, public WIFI areas, hotel/train broadband connections etc.

- The user is responsible for maintaining their home working environment in conformance with the practice's requirements for home working such as, but not limited to, Health & Safety, Display Screen Equipment (DSE) assessments, manual handling, fire safety, security of the premises, insurance, other individuals who have access to the area where the remote access is taking place, etc.
- The user is responsible for preventing compromise of the data they are working on and avoiding the use of unauthorised or unlicensed software that may contain a virus, spyware, malware or other malicious code.
- The user must make sure that a current operating system and appropriate anti-virus, anti-spyware & firewall software products are installed on the remote PC/laptop and they are kept up to date. This will be confirmed and documented in the Home Risk Assessment Survey carried out by the practice for each remote access user.
- The user is responsible for ensuring that the remote PC/laptop and/or its hard drive is disposed of securely at the end of its useful life via the NECS hardware disposal service.
- The user must read the Connecting for Health guidance on safe computing use
- The user named below has read, understood and agrees to the Terms & Conditions of use of the remote working solution (AFMD Biometric Edition).
- Each user of this system, AFMD Biometric Edition, needs to sign this document.

Please note that by listing the individual user details on the spreadsheet, you are affirming their compliance with the above terms and conditions.