

Digital Application Portal

Minimum User Requirements

1. Purpose

This document explains what users need to access and use The Digital Application Portal. The Digital Application Portal is a web application and therefore it is browser-based, mobile responsive, and designed to support the application process for individuals applying for a position on a Non-Medical Prescribing Course.

This document is intended as general user guidance and minimum technical guidance only. It is intended to help users access the platform reliably and securely. It does not replace any local IT, information governance, accessibility, employment, university, Trust, organisational or professional requirements that may also apply.

2. General Requirement

Users must access the platform using a device, operating system and web browser that are still supported and able to receive security updates.

For security and compatibility reasons, users should keep their device, operating system and web browser up to date.

The Digital Application Portal is designed to work with current, supported browsers and operating systems.

3. Devices

The Digital Application Portal can be accessed using:

- Desktop computers and laptops
- Tablet computers
- Smartphones

The platform is mobile responsive and is designed to adapt to different screen sizes; however, users may find a laptop, desktop computer or tablet more suitable than a smartphone.

4. Operating Systems

Users should use a currently supported version of one of the following operating systems:

- Microsoft Windows;
- macOS;
- iOS or iPadOS;
- Android;
- ChromeOS; or
- a mainstream Linux distribution capable of running a current supported web browser.

Unsupported operating systems should not be used to access The Digital Application Portal.

5. Browsers

Users must use a current, supported version of one of the following browsers:

- Google Chrome;
- Microsoft Edge;
- Mozilla Firefox; or
- Apple Safari.

The browser must be kept up to date and must support modern web standards, including HTML5, CSS3, JavaScript, and secure HTTPS connections.

The following are not supported:

- obsolete/discontinued browsers;
- heavily restricted in-app browsers;
- browsers blocked by local IT settings;
- browsers with extensions or settings that stop the Digital Application Portal working properly.

For the best experience, users should open the Digital Application Portal directly in their browser rather than an email preview.

6. Browser Settings

For the platform to function correctly, users must ensure that:

- JavaScript is enabled;
- cookies are enabled;
- pop-ups are allowed where required for course content, resources or external links;
- PDF files can be opened or downloaded where required;
- audio and video playback is permitted where used within course content;
- browser extensions, ad blockers or privacy tools are not blocking essential platform features.

If a user experiences problems, they should first try updating their browser, clearing their browser cache, or disabling conflicting extensions.

7. Internet Connection

Users require a stable internet connection.

As a general minimum, users should have a connection suitable for loading webpages, submitting and accessing documents and opening external links.

The Health & Education Co-operative cannot guarantee uninterrupted access especially where a problem is caused by the user's device, internet connection, local network, browser settings, firewall, local IT restrictions or a third-party service.

8. Documents, Downloads and External Links

The Digital Application Portal requires users to click on links to access relevant sections of the application and to upload evidence (documents and images).

Users are responsible for ensuring their device has suitable software or browser capability to open any required files. Access to external websites may depend on the availability, security settings and accessibility of those third-party websites, which are outside the direct control of The Health & Education Co-operative LTD.

The platform provider is not responsible for the content, availability or technical performance of third-party websites unless otherwise expressly stated.

9. Accessibility

The platform is intended to support access by users with a range of needs and should be used with current assistive technologies where required, such as screen readers, browser zoom, speech recognition tools or operating system accessibility features.

Users should ensure they are using up-to-date assistive technology and a supported browser/operating system combination.

Where users require additional support or alternative formats, they should contact the university they are applying to, their NMP Lead/Supervisor, or our support team.

10. Security

Users should access the platform using a secure device, operating system and browser that are still supported and able to receive security updates.

Users should not knowingly access the platform using a device or browser that is insecure, compromised, unsupported, or no longer receiving security updates.

Where a device is managed by a university, Trust, employer or other organisation, responsibility for updates, security settings, anti-malware protection and device management may sit with that organisation's IT team. Users should follow their organisation's local IT and information governance policies.

Users are responsible for taking reasonable steps within their control to keep access secure. This includes:

- keeping login details confidential;
- not sharing accounts;
- signing out when using a shared or public device;
- reporting suspected account or security issues promptly;
- avoiding public or untrusted devices when accessing personal, course or learner information;
- following any local IT, information governance, assessment or acceptable use policies that apply to them.

Where users are able to manage their own device, they should also:

- install operating system and browser updates promptly;
- use appropriate anti-malware or endpoint protection where appropriate;
- keep their device protected with a password, PIN, biometric login or similar security measure.

11. Shared or Public Devices

If using a shared computer or public computer, users should:

- sign out of their Digital Application Portal account after use;
- delete downloaded files where appropriate;
- avoid leaving personal, course or learner information visible.

12. Email and Notifications

Users must have access to the email account linked to their Digital Application Portal account. This is required for account activation, password reset links, activity and application form progress-related emails and similar relevant system emails.

Users should check their junk or spam folder if expected emails do not arrive.

Organisations using managed email systems should make sure Digital Application Portal emails are not blocked, quarantined or filtered by local email security rules.

13. Things outside our control

We will make reasonable efforts to support access to The Digital Application Portal using current mainstream browsers and supported operating systems. However, we cannot guarantee that The Digital Application Portal will work perfectly on every device, browser, network or local setup.

Access may be affected by:

- poor or unstable internet connection;
- local firewall,VPN or proxy settings;
- browser extensions or restrictive browser settings;
- Old software or unsupported devices;
- managed device restrictions;
- organisation IT policies and security controls;
- public Wi-Fi;
- third-party website issues;
- third-party service interruptions
- local device faults;
- endpoint security software
- incorrect settings or user actions.

If you have any questions about the guidance in this document, please contact us.