

SN@P Minimum User Requirements

1. Overview

This document explains what users need to access and use SN@P.

SN@P may be used for mock/formative assessments, summative assessments, learner feedback, viewing educational materials and related learning and assessment activities.

Some assessments may also be remotely invigilated using SN@P's Invigilation Centre. Where this applies, users must also meet the Zoom invigilation requirements set out in this document.

This document is intended as general user guidance and minimum technical guidance only. It does not replace any assessment rules, university policies, employer policies, professional requirements, reasonable adjustment arrangements or invigilation instructions that may also apply.

2. Main requirement

Users should access SN@P using a device, operating system and web browser that are still supported and able to receive security updates.

Users should keep their device, browser and operating system up to date.

SN@P is designed to work with current, supported browsers and operating systems.

3. Devices

SN@P can be accessed using:

- Desktop computers and laptops
- Tablet computers
- Smartphones

For assessments, revision practice quizzes and invigilated sessions, we strongly recommend using a laptop or desktop computer.

Phones and tablets may work for some activities, but they are not always suitable for formal assessments because of their smaller screen size. If an academic gives specific device instructions, those instructions must be followed.

4. Operating systems

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

- Microsoft Windows;
- macOS;
- iOS or iPadOS;
- Android;
- ChromeOS; or
- a mainstream Linux distribution that can run a current supported browser.

Unsupported operating systems should not be used to access SN@P, especially where assessment data, learner records or personal data may be involved.

5. Browsers

Users should use the latest version of one of these browsers:

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

The browser must support modern web standards, including JavaScript, cookies and secure HTTPS connections.

SN@P does not support:

- obsolete/discontinued browsers (e.g. IE 8);
- heavily restricted in-app browsers;
- browsers blocked by local IT settings;
- browsers with extensions or settings that stop SN@P working properly.

For the best experience, users should open SN@P directly in their browser rather than an email preview.

6. Browser settings

To use SN@P properly, users should make sure that:

- JavaScript is enabled;
- cookies are enabled;
- pop-ups are allowed where needed;
- Word Documents and PDF files can be opened or downloaded where needed;
- audio and video can play where used;
- browser extensions are not blocking essential features.

If SN@P does not work as expected, users should try:

- updating their browser;
- clearing their browser cache;
- disabling browser extensions that may be interfering;
- using a different supported browser;
- restarting their device.

7. Internet connection

Users need a stable internet connection.

Users should only start an assessment when they are reasonably confident their device and internet connection are working properly.

For assessments, users should use a stable broadband or strong Wi-Fi connection where possible. Public Wi-Fi, weak Wi-Fi signal or mobile data may increase the chance of disconnection.

SN@P 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. Before starting an assessment

Before starting an assessment users should check that:

- their device is charged or plugged in;
- their internet connection is stable;
- they have enough time to complete the activity;
- they have read the assessment instructions;
- they have closed unnecessary browser tabs and applications;
- they are in a suitable distraction-free place to complete the activity.

Users should not start an assessment if they already know there is a technical issue that may stop them completing it. If a technical problem happens during an assessment, users should follow the instructions given by their university, employer, assessment organiser or invigilator.

9. Screen size

SN@P is fully responsive and designed to work across different screen sizes.

However, for formal assessments, a larger screen is strongly recommended.

A laptop or desktop screen will usually give a better experience than a phone.

Small screens may make it harder to read questions, review answer options, check calculations or view feedback.

10. Documents and external links

SN@P may include documents, PDFs, videos, images, downloads or links to external websites.

Users are responsible for making sure their device can open any required files.

External websites are outside the direct control of the SN@P platform provider. We cannot guarantee that external websites will always be available, accessible, secure or compatible with every device.

11. Accessibility and reasonable adjustments

SN@P is intended to support access for users with a range of needs.

Users may use suitable assistive technology, such as:

- screen readers;
- browser zoom;
- speech recognition software;
- operating system accessibility tools;
- contrast or display settings.

Users should use up-to-date assistive technology with a supported browser and operating system. If a user needs reasonable adjustments, extra time, alternative formats or support with access, they should contact their university, employer or assessment organiser in advance. Users should not wait until the start of an assessment to raise known access needs.

12. Security

Users should access SN@P using a secure device, operating system and browser that are able to receive security updates.

Users should not knowingly access SN@P 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, assessment, quiz or learner information;
- following any local IT, information governance, assessment, academic integrity 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.

Users must not try to bypass SN@P controls, access another user's account, copy assessment content, interfere with an assessment, or use SN@P in a way that breaches assessment rules, academic integrity requirements, acceptable use policies or the law.

13. Shared and public devices

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

- sign out of their SN@P account after use;
- delete downloaded files where appropriate;
- avoid leaving personal or assessment information visible.

14. Email access

Users must have access to the email account linked to their SN@P account. This is required for account activation, password resets, assessment information, and receiving responses from our support team.

Users should check their junk or spam folder if expected emails do not arrive. Organisations using managed email systems should make sure SN@P emails are not blocked, quarantined or filtered by local email security rules.

15. Things outside our control

We will make reasonable efforts to support access to SN@P using current mainstream browsers and supported operating systems. However, we cannot guarantee that SN@P 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.

16. Zoom invigilation requirements

Some SN@P assessments may be remotely invigilated by SN@P's Invigilation Centre which uses Zoom video conferencing technology.

Where invigilated assessments are required, users must follow the instructions provided by their university, employer, assessment organiser or invigilator.

A stable upload and download connection is required. The minimum download speeds below are intended to support the SN@P invigilation process and may be higher than Zoom's general minimum requirements.

Minimum requirements for Learners:

Device	Type	Requirements
Device 1	Desktop Computer or Laptop	• Good internet connection (Wi-Fi or wired connection) • Minimum download speed of 15 Mbps. • Permissions to screen share
Device 2	Smartphone	• Must have a functioning camera, microphone and speaker(s). • Connected to the internet (Wi-Fi or Cellular). • Capable of receiving text messages. • Have the "Zoom Workplace App" installed.

Device 1 is the device you will take your exam on.

Device 2 is the device your invigilators will use to monitor you.

Minimum requirements for Invigilators:

Device	Type	Requirements
Device 1	Desktop Computer or Laptop	• Good internet connection (Wi-Fi or wired connection) • Minimum download speed of 30 Mbps. • Google Chrome or Microsoft Edge browser • A functioning camera and microphone

Invigilators require a good download speed (30 Mbps minimum) and strong signal if you are connected to Wi-Fi to view multiple learners at the same time.

For remote invigilation, learners are expected to:

- keep their camera on;
- keep their microphone on;
- share their screen (full-screen share);
- show their photo ID;
- show their working environment (desk/table space and room in a 360 sweep).
- position a second device so the invigilator can see them and their screen;
- remain visible to the invigilator during the assessment.

Users should test that the SN@P Invigilation solution works before their first assessment session. To do this, they should make sure the Zoom app is installed, up to date and allowed to use the camera and microphone.

Users should not rely on a work device, managed device, locked-down device or public device unless they know it allows Zoom, camera access, microphone access and screen sharing. If a user cannot meet the Zoom invigilation requirements, they should inform the person who asked them to take the assessment as soon as possible.

If the invigilation requirements cannot be met, the assessment may need to be delayed, rearranged or managed in line with the organisation's assessment process.

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