

SN@P Acceptable Use Policy

Purpose

This Policy is designed to keep SN@P safe, fair and secure for everyone. It also helps protect learner accounts, assessment integrity, platform content and personal data.

This Policy applies to anyone who accesses SN@P. This includes users who have purchased an individual licence and users who have been given access by their employer, university, NHS Trust, organisation or educational institution. It also applies to learners, academics, assessors, invigilators, administrators and anyone else using SN@P on behalf of an organisation.

In this Policy, “learner” means anyone using SN@P to complete learning activities, revision resources, practice questions or assessments. This includes university students, employees, trainees and individuals using a personal licence.

This Policy, its subject matter and its formation are governed by English law. You and we both agree that the courts of England and Wales will have exclusive jurisdiction.

Acceptable Use

SN@P should only be used for legitimate learning, assessment, training, revision, support or administrative purposes. You may use SN@P to complete the assessments, learner journey modules, watch tutorial videos and complete other activities and tasks that are relevant to your account, course or organisation.

You must follow any instructions provided by SN@P, The Health & Education Co-operative Ltd, your university, employer, Trust, organisation or invigilator where those instructions relate to your use of SN@P.

Account Security

SN@P accounts are for individual use.

You must not share your account, login details, password or two-factor authentication code with anyone.

Our staff and contractors may ask you to confirm information such as your email address, cohort details or organisation. We will never ask you to disclose or share your password.

You should tell us as soon as possible if you believe your account has been accessed by someone else, your password has been shared or exposed, or your account activity does not look right. This helps us protect your account and review any activity that may have taken place.

SN@P may temporarily restrict or block access during lengthy periods of inactivity or where suspicious login activity, unusual account activity or a possible security risk is detected. This may happen without advance notice where we believe it is necessary to protect users, data, assessment integrity or the platform. Where an account is restricted or blocked without advance notice, we will endeavour to contact the user as soon as reasonably practicable thereafter to explain the restriction, unless we are prevented from doing so by law, regulatory obligation, or ongoing security investigations.

Assessment and Academic Integrity

SN@P assessment content must be treated as confidential.

You must not copy, photograph, screenshot, record, share, publish, publicly post, sell, transfer, reproduce, alter or distribute assessment questions, answers, feedback, learning content or other SN@P materials. You must not use SN@P in a way that supports cheating, impersonation, unauthorised assistance, collusion or any other activity that could undermine assessment integrity.

This includes, but is not limited to:

- attempting to access assessments or content that you are not authorised to access;
- sharing answers, questions, screenshots, recordings or assessment content with another person;
- asking another person to complete an assessment on your behalf;
- completing an assessment on behalf of another person;
- using unauthorised materials, software, artificial intelligence tools, messaging apps, websites or other assistance during an assessment where this is not permitted;
- interfering or attempting to interfere with assessment settings, timers, results, feedback, invigilation or platform controls.

Invigilated assessments

If you are taking an invigilated assessment, you must read the relevant guidance before the assessment and follow the instructions given by SN@P, the invigilator and your organisation.

This may include requirements relating to your device, browser, internet connection, camera, microphone, screen sharing, room setup, identification checks, 360-degree room checks and conduct during the assessment.

The latest minimum requirements and invigilated assessment guidance are available on our website: <https://www.hecooperative.co.uk/minimum-requirements/>

Failure to follow invigilation instructions may affect whether your assessment can be completed, reviewed or accepted by your organisation.

Devices, Browsers and Internet Connection

You are responsible for accessing SN@P using a suitable, secure and supported device, browser, and a stable internet connection.

Where your device is managed by a university, Trust, employer or other organisation, local IT settings may affect your ability to access SN@P, screen sharing or other required features. You should follow your organisation's local IT and information governance policies. If you are able to manage your own device, you should keep your operating system and browser up to date and avoid using devices or browsers that are unsupported/obsolete.

Content Uploaded or Entered by Users

You must only enter content into SN@P that is appropriate, lawful, relevant and accurate to the best of your knowledge.

This applies to assessment answers, learner evaluations, feedback, support tickets, question banks, learner journeys and any other text, files or content added to SN@P.

You should avoid entering unnecessary personal, confidential or sensitive information. If you are an administrator or academic user, you must take particular care when entering or uploading information about learners or other individuals.

Users who add their own content to custom question banks, learner journeys or other areas of SN@P must ensure they have the right to use that content.

You must not upload, post, publish or transmit material that infringes copyright, intellectual property rights, confidentiality obligations or the rights of another person or organisation.

The Health & Education Co-operative Ltd does not routinely monitor, endorse or verify text, files or materials uploaded or entered into SN@P by users.

Users are responsible for ensuring that any content they add is lawful, appropriate and that they have the right to use it. If user-generated content causes a legal, confidentiality, data protection or intellectual property issue, we may remove or restrict access to that content and may take other appropriate action.

Intellectual property and confidential information

Unless stated otherwise, SN@P content, assessment materials, learning materials, platform design, text, images, videos, documents, question banks and other materials are owned by or licensed to The Health & Education Co-operative Ltd.

You are given access to SN@P only for the purposes allowed by your account, licence, course or organisation. Access to SN@P does not give you ownership of, or any wider rights to use, copy, reproduce, publish, distribute, sell, adapt, share or reuse SN@P content. No other rights are granted.

You must not use SN@P content for any purpose other than the purpose for which access was provided. You must not disclose SN@P content or confidential information to another person or organisation unless you are authorised to do so or required to do so by law.

Confidential information does not include information that is already public, information you lawfully had before it was disclosed to you, or information that must be disclosed by law, court order, regulatory body or other lawful authority.

Prohibited Use

You must not use SN@P in a way that is unlawful, unsafe, harmful, misleading or likely to affect the security, availability, integrity or performance of the platform.

You must not:

- attempt to gain unauthorised access to SN@P, another account, assessment content, learner data, servers, systems, databases or connected services;
- attempt to bypass, disable, interfere with or test SN@P security controls, access controls, assessment controls, invigilation controls or platform restrictions without permission;
- introduce viruses, malware, trojans, worms, logic bombs, spyware, adware, bots, keyloggers or any other harmful code or material;
- use automated tools, scraping, bots, scripts or similar methods to access, copy, extract or interfere with SN@P unless we have given written permission;
- copy, reproduce, store, publish, display, retransmit, distribute, sell, transfer, adapt or reuse SN@P content unless you have clear permission to do so;
- send communications to our staff or other users that are abusive, threatening, discriminatory, defamatory, obscene, harassing, knowingly false, illegal or likely to cause needless distress;
- upload or enter content that is unlawful, inappropriate, offensive, discriminatory, defamatory, malicious, misleading or infringes another person's rights;
- use SN@P to facilitate or carry out illegal activity.

Monitoring and Security

SN@P may record activity such as login events, assessment activity, timestamps, IP addresses, device or browser information, administrative actions and other audit information.

We use this information for purposes such as security, support, troubleshooting, platform administration, assessment integrity, fraud prevention and investigating suspected misuse. More information about how personal data is used is available in our Privacy Policy.

Reporting Concerns

You should contact us as soon as possible if you become aware of a security concern, suspected account misuse, suspected data issue, technical problem, assessment irregularity or possible breach of this Policy.

If your access was provided by your university, employer, Trust or organisation, you may also need to report the issue through their local process.

Consequences of misuse

We review misuse, suspected misuse and suspicious activity on a case-by-case basis. We will take a proportionate approach based on the nature of the concern, the evidence available, the risk to users, the risk to assessment integrity and the risk to SN@P and The Health & Education Co-operative Ltd.

Suspected misuse may result in temporary restriction or suspension while we review the matter. Where appropriate, we may contact you for more information.

Where your access was provided by a university, employer, Trust or organisation, we may notify an appropriate key contact at that organisation. This may include relevant information about the suspected misuse, assessment activity or account activity where it is appropriate and lawful to do so.

Where there is evidence of misuse, we may take action.

This may include keeping the restriction in place, closing the account, withdrawing access, invalidating or flagging assessment activity, notifying the relevant organisation, or taking other steps that are necessary to protect users, assessment integrity, personal data or the platform.

Nothing in this Policy prevents us from taking urgent action where we reasonably believe it is necessary to protect SN@P, users, personal data, assessment integrity or platform security.

Severability

If any provision or part-provision of this Policy is or becomes invalid, illegal, or unenforceable under the laws of England and Wales, it shall be deemed deleted. However, this shall not affect the validity and enforceability of the rest of this Policy, which will remain in full force and effect.

Relationship with other policies

This Policy does not replace any exam conditions, professional standards, academic regulations, employment policies, information governance requirements or local rules set by your university, employer, Trust or organisation.

You should read this Policy alongside our Privacy Policy, Minimum User Requirements, assessment guidance, invigilation guidance and any local policies that apply to you.

Review

We may update this Policy from time to time to reflect changes to SN@P, legal requirements, security expectations or assessment processes.

Last Reviewed: June 2026