

Simplified User Guide & Checklist





Claims Portal User Agreement for Claims Handlers/Team Leaders

All Claims Portal users should consider if they can answer 'yes' to the following questions to ensure ongoing adherence to the Claims Portal user Agreement. Failure to do so may make Portal data and user profiles accessible to unauthorised parties.

- Do you have your own credentials to access the Claims Portal?
- Do you know your user name and password? You must not write these down or save them to your PC outside of secure digital password manager tools (e.g. NordPass).
- Have you verified your user credentials for Multi Factor Authentication using a business email address accessible only by you?
- Are you aware of your organisation's information security policies and procedures?
- Are you aware of the Claims Portal User Guides available on the Claims Portal website?

<https://www.claimsportal.org.uk/>



Claims Portal User Agreement for Administrators

Administrators should consider if they can answer 'yes' to the following questions to ensure ongoing adherence to the Claims Portal user Agreement. Failure to do so may result in delays in correspondence with Claims Portal, including service updates.

Account Management

- Are your registered Organisation's contact details up to date on the Claims Portal?
- Is your organisation's account registered using a generic business email address?
- Are your individual Portal users aware of the General Conditions of Use for Portal Users?
- Are you aware of the URL for the full User Agreement?

<https://www.claimsportal.org.uk/media/2841/combined-portal-user-agreement-14-sept-2018.pdf>



Claims Portal User Agreement for Administrators

Administrators should consider if they can answer 'yes' to the following questions to ensure ongoing adherence to the Claims Portal user Agreement. Failure to do so may make Portal data and user profiles accessible to unauthorised parties.

Profile Management

- Have you created individual access credentials for each Portal user at your organisation?
- Has each user verified their credentials for Multi Factor Authentication using an individual business email address?
- Do you disable access to the Portal immediately when a user leaves the organisation or no longer requires Portal access?
- Do you review the user profiles at least quarterly to check that only those currently requiring access to the Portal have active and enabled credentials and that the expiry dates and passwords are current?



Audit Rights and Remediation

- Claims Portal User Access audits are performed by the Claims Portal Audit Team ("CPAT"), which is managed by the Motor Insurers' Bureau ("MIB")
- Co-operation with the CPAT is required under the terms of the User Agreement
- The audit shall review each User Organisation's adherence to the requirements highlighted in this User Guide.
- Where instances of non-compliance are identified, User Organisations will be required to evidence their remediation of such items within agreed timescales, and the Claims Portal Board shall be made aware of User Organisations who fail to do so
- Full details of the audit approach can be found in the Claims Portal Audit Guide