

Privacy Notice – Dual Factor Authentication

The traditional use of Passwords to authenticate an individual has long been recognised as being a vulnerability to threat actors. These are becoming more easily compromised through a variety of means and global experience has shown that this could have a devastating impact on UNE. Multi Factor Authentication (MFA) is the recommended solution to address this issue, both by the global security community and endorsed by ACSC. All University users and assets must be uniquely identified and validated before gaining access to UNE resources. For human users, user validation will be by means of 'Multi-Factor Authentication' using unique security 'tokens'. This allows us to better protect your personal information and UNE resources.

Authentication of the user is done using a secure 'App' installed on the user's smartphone from either the Android or Apple stores.

The information you provide is collected by the University of New England and third party representatives to authenticate users and to provide access. The University abides by the *Privacy and Personal Information Protection Act 1998* NSW (PPIP Act) as outlined in the [UNE Privacy Management Plan](#).

What kinds of personal information is collected?

We will collect your name, mobile number and geographic location.

What happens if I do not wish to provide my personal information?

If you do not wish to disclose personal information at this time, the University cannot provide access to UNE systems. In some circumstances it may be possible to authenticate via a hardware token if mobile phone App authentication is impossible.

How will my information be used and with whom will it be shared?

Only authorised UNE staff members and representatives will have access to your personal information. Information is used to provide access to UNE systems and services by authenticating users. Location information for example helps to ensure that your login location and that of your mobile phone match and helps to flag unusual or suspicious activity.

Where will my information be stored?

Your personal information will be stored securely in accordance with the *PPIP ACT* within Australia.

When no longer required, UNE will destroy or archive personal information in a secure manner in accordance with the *PPIP Act* and the *State Records Act, NSW 1998*.

How can I access or correct my information?

You can request access to the information UNE holds about you, by contacting People and Culture.

Details on the management of personal information at UNE can be found in the [Privacy Management Plan](#), for further information regarding privacy please contact the UNE Privacy Officer via privacy@une.edu.au.