

Multi-Factor Authentication (MFA) Privacy Considerations

Frequently Asked Questions

What about my privacy? Why do I have to provide personal contact details for MFA?

UC has carefully assessed the risks and benefits of introducing MFA. We consider that this is necessary to use MFA to ensure appropriate security of UC systems. This safeguards the interests of UC and all its system users, as a cyber security incident could result in loss of personal information of UC students and staff, lock users out of UC systems and disable key operations. The MFA process must, by definition, use information which is personal to you or personally accessible only to you.

How is my personal data stored?

The personal details you share are used solely for the purpose of identity verification and authentication, which you can find more information [here](#).

Data jurisdiction

Any data you provide is housed with the UC Azure Tenancy, which is based in Australia.

Who will be able to see the information I provide?

The details you provide will always be kept securely and only used for authentication. They can only be accessed by you as an individual or by UC privileged administrators who will only do so if they need to support you in resolving an issue relating to these services (except that any answers you provide for security questions will not be available to the administrators, only to you). Further privacy information is available [here](#).

How does the University store my information?

The personal details you provide when you set up Multi-Factor Authentication are held securely within Microsoft's systems and only you can view your full data.

Why is personal information required?

To prove your identity to the system, the information you provide needs to be unique to you, for example, an email address.

We recommend that you use the [Microsoft Authenticator app](#) to authenticate wherever possible, as this allows for personal verification while reducing the amount of personal contact information you need to provide.

Privacy statement

Private information at the University of Canterbury is managed in line with both the Privacy Policy and the Privacy Declaration. Both of these can be viewed in full on the [Privacy Obligations](#) page.

In the event of any security/privacy breach from Microsoft the University will be informed and this will be managed through our Breach Response Plans. If your data is affected you will be informed.

If you have any questions or concerns relating to your personal data and how it is used, please contact privacy@canterbury.ac.nz