INFORMATION AND COMMUNCIATIONS TECHNOLOGY
MULTI-FACTOR AUTHENTICATION (MFA) PRIVACY NOTICE

The University of Sydney is committed to protecting your privacy and processing your personal information fairly and lawfully, in compliance with the NSW *Privacy and Personal Information Protection Act* 1998 and the NSW *Health Records and Information Protection Act 2005* and also the General Data Protection Regulation 2018, as applicable.

Multi-factor authentication (MFA) is an important tool that helps the University to manage its cyber security risks. MFA allows the University to add an extra layer of security, to verify an end user's identity when they sign into an application. This additional layer of security helps to protect University systems and the data they contain from unauthorised uses and attacks. The University is using third-party service provider, Okta, to help administer multi-factor authentication (MFA).

In order to provide these security controls, some personal information about you will be collected and used through the University's MFA processes. You will be asked to provide some personal information when registering for MFA services, such as a mobile number and work email address. Other administrative information about your ICT system profiles will also be shared with Okta. Audit logging and security monitoring and alerting will also be used in the University's MFA environment to help protect against unauthorised access and potential cyber-attacks.

The personal information collected and used during MFA processes is necessary to administer and monitor access to University applications. The personal information associated with MFA processes will only be used by authorised systems and staff for the purpose of monitoring and maintaining system access and security.

To make using MFA processes more seamless, staff and students are encouraged to download the Okta Verify app. In order to manage your access to University applications, this app will collect the following information. This information is required to support the push notification feature of Okta Verify and provide administrators with the detail required to manage multiple Okta Verify tokens per user. This data is encrypted and stored within the University's Okta tenant:

- the IMEI (International Mobile Equipment Identity)
- device name
- device type
- OS version
- serial number
- and push notification details (originating IP and geolookup).

You are also able to use Google Authenticator for the University's MFA processes. Google Authenticator will use your Google account to transmit verification codes to you when required for MFA processes. Information from your Google account will not be shared with the University but your authenticated access into University systems will be logged.

The University will not disclose your personal information to anybody else without your consent, unless we are authorised or required to do so by law. The University and its partner Okta will also take all reasonable steps to ensure that the personal information we hold for MFA processes is accurate and complete, and that appropriate technical and organisational security measures are in place and maintained to protect your personal information from accidental or unlawful destruction, misuse, loss, alteration, unauthorised access or disclosure.

Information provided for MFA will only be retained for as long as it is required to enable you for ongoing authentication to use University applications, and in accordance with our legislative obligations.

This information will then be securely destroyed in accordance with the University's legal requirements under NSW State Records legislation.

You have the right to access and correct your personal information held by the University. Should you wish to access or amend your information please contact the ict.helpdesk@sydney.edu.au

This privacy statement should be read in conjunction with the Privacy Policy which describes how the University handles personal information.