



Privacy - it's all about you

ANU recognises that privacy is very important.

The way we collect, use, disclose, secure, and dispose of personal information is governed by our compliance with, and obligations as an 'agency' under the Privacy Act 1988 (Cth), including the Australian Privacy Principles (APPs).

New privacy laws: what you need to know

Australia is undergoing significant changes to its privacy laws, aimed at enhancing the protection of personal data and ensuring greater transparency in how information is handled.

Changes include the introduction of new civil penalties for serious privacy breaches. This means if the University mishandles personal data, it could face substantial fines, emphasising the importance of robust data protection measures.

Another notable reform is the introduction of a statutory tort for serious invasions of privacy. This provides individuals with a legal avenue to take action if their privacy is significantly violated. With increasing privacy awareness, it is likely that individuals will seek to exercise their legal rights for privacy infringements.

The Australian Government is also implementing a 'right to be forgotten,' allowing individuals to request the deletion of their personal data under certain circumstances.

These changes are designed to empower individuals with greater control over their personal information and increases the University's accountability around our data practices.

The ANU Privacy Office will be developing an implementation plan that will ensure the University meets all new obligations and that staff receive the appropriate training and support as changes are implemented.

Reporting privacy breaches: new web form

The ANU Privacy Office is excited to [introduce a new web form](#), designed to streamline the process of reporting privacy breaches. This tool is part of our ongoing commitment to safeguarding personal data and ensuring compliance with the latest privacy regulations.

A privacy breach occurs when personal information is accessed, disclosed, or lost in a way that compromises its security. This can include unauthorised access to personal information, accidental sharing of personal information, or loss of devices containing information. Such breaches can have serious consequences, including identity theft, financial loss, and damage to an individual's reputation.

Our new web form makes it easier for staff, students and members of the community to report any suspected privacy breaches quickly and efficiently. The form is user-friendly and guides you through the necessary steps to provide detailed information about the incident. This includes describing the nature of the breach, the type of data involved, and any immediate actions taken to mitigate the impact.

By promptly reporting privacy breaches, you help us take swift action to address the issue and prevent further harm. The information collected through the web form will enable our compliance team to investigate the breach thoroughly and implement measures to prevent future occurrences.

Reporting potential data breaches is crucial for maintaining the highest standards of data protection.

AI and protecting personal information

As we increasingly rely on AI tools to enhance our productivity, it's crucial to remember the importance of safeguarding personal information. AI systems, while powerful and efficient, are not immune to security risks. Entering personal data into AI applications can expose sensitive information to unauthorised access and potential misuse.

Personal information includes details such as name, address, phone number, email, financial information, and any other data that can identify an individual. Sharing this information with AI tools, especially those not specifically designed for secure data handling, can lead to privacy breaches and identity theft.

To protect your privacy and that of others, always avoid inputting personal information into AI systems. If you are drafting emails or documents, identifying details should not be included in AI prompts, and added manually to the AI output. If you have any doubts about the security of an AI tool, contact the ANU ServiceDesk for guidance.

Your vigilance in protecting personal data helps maintain our commitment to privacy and security.

What is the leading cause of data breaches?

Did you know that email errors are the most common cause of data breaches at the University?

Simple mistakes, such as sending an email to the wrong recipient or attaching the wrong file, can lead to significant privacy violations and data loss. These errors can expose sensitive information, including personal details, financial data, and confidential business information.

To minimise the risk of email-related data breaches, it's essential to double-check the recipient's address before hitting send. Keep in mind that there may be more than one person with the same name, so care should be taken when selecting emails from the global directory. Always verify that the correct files are attached and ensure you are only sharing personal information that is necessary and appropriate. Additionally, be cautious when using the "Reply All" function, as it can inadvertently share information with unintended recipients.

By adopting these best practices, we can significantly reduce the likelihood of email errors and protect the University's data. Your attention to detail is crucial in maintaining our commitment to privacy.

Looking for more privacy advice?

For assistance with any privacy questions please visit the [ANU Privacy website](#) or reach out to the [ANU Privacy team](#). They are here to support any privacy needs and can provide a customised information session for your local area.



ANU Privacy Policy

Learn about the [University's personal information handling practices](#)



Training & resources

Access [training modules, online resources and additional support](#)



Privacy FAQs

Read responses to [frequently asked questions about privacy](#)

Contact

+61 2 6125 4679
privacy@anu.edu.au
anu.edu.au/privacy

The Australian National University,
Canberra

CRICOS Provider : 00120C
ABN : 52 234 063 906

If you do not wish to receive future emails from us, please [contact the Privacy Office](#)

