Australia and New Zealand
Transplant and Cellular Therapies

DIGITAL RESPONSIBILITY, SOCIAL MEDIA & CYBERSECURITY POLICY

Australia and New Zealand Transplant and Cellular Therapies Ltd (ANZTCT) values a professional, secure, and respectful digital environment. This policy sets expectations for responsible use of social media, electronic communication, internet services, and devices when working with or representing ANZTCT. It promotes a culture of integrity, transparency, and cyber safety.

ANZTCT recognises that digital tools are integral to modern work and communication. This policy balances individual autonomy with the organisation's obligation to protect confidential information, digital systems, and professional reputation.

All employees, contractors, and volunteers must:

- Act in alignment with ANZTCT's values when using electronic communication or digital systems
- Take reasonable steps to protect ANZTCT's systems, information, and reputation
- Use professional judgment when engaging with digital or social media platforms

In so far as this policy imposes any obligations on ANZTCT, those obligations are not contractual and do not give rise to any contractual rights. To the extent that this policy describes benefits and entitlements for employees, they are discretionary in nature and are also not intended to be contractual. The terms and conditions of employment that are intended to be contractual are set out in your written employment contract.

The ANZTCT may unilaterally introduce, vary, remove or replace this policy at any time.

EMAIL AND INTERNET USE

ANZTCT acknowledges the necessity of using the internet and email for work duties. This policy applies when accessing ANZTCT systems:

- On site or offsite
- During or outside of work hours
- On personal or ANZTCT-issued equipment

All files, emails, and systems accessed through ANZTCT infrastructure are the property of the organisation. Employees must:

- Use systems only as required for work duties
- Follow any guidance issued by ANZTCT
- Provide all passwords and return all materials (e.g. laptops, USBs) upon request or upon ceasing employment or engagement

As far as reasonably possible, ANZTCT will respect individual privacy while ensuring safe operations.

Prohibited Conduct:

- Sending defamatory, threatening, offensive, or sexually explicit material
- Sharing or downloading discriminatory, obscene, or unlawful content
- Using ANZTCT systems to hack or access unauthorised information
- Deleting or modifying ANZTCT data without permission
- Binding ANZTCT to legal obligations without authorisation
- Disclosing confidential information unless required for duties

SOCIAL MEDIA PARTICIPATION

ANZTCT supports responsible social media engagement that reflects positively on the organisation. The following rules apply whether using social media during or outside work hours, and whether on ANZTCT or personal devices:

All employees and volunteers must:

- Not refer to ANZTCT, its staff, or stakeholders without express permission
- Not imply they speak on ANZTCT's behalf unless authorised
- Avoid posts that bring ANZTCT into disrepute
- Not post criticism or disparagement of ANZTCT or its people
- Ensure online activity does not impair work performance
- Not suggest ANZTCT endorses personal opinions
- Not disclose confidential information
- Not share photos or content related to ANZTCT work or premises without permission
- Not harass, discriminate, or bully through social media

Where permission has been granted to post as a representative of ANZTCT, content must reflect ANZTCT's values and approved messaging.

CYBERSECURITY AND DEVICE USE

Every team member contributes to cybersecurity. The following practices are expected:

Secure Access:

- Use strong passwords and enable two-factor authentication
- Lock devices when unattended
- Report lost/stolen devices or suspicious activity immediately

Personal Devices:

- Must have updated antivirus, OS patches, and password protection
- Should only be used to access ANZTCT systems via secure methods

Email Safety:

- Do not click suspicious links or download unauthorised files

- Never forward sensitive information to personal accounts

BREACHES

Breaches of this policy may result in corrective action, including restricted access, education, or disciplinary processes. Serious violations—especially those involving cybersecurity threats or reputational damage—may result in termination of engagement and/or reporting to authorities.

OTHER POLICIES

Employees are encouraged to read this policy in conjunction with other relevant Company policies, including:

- Code of Conduct
- Workplace Anti-Bullying & Anti-Harassment Policy
- Acceptable Use of Electronic Media Policy
- Equal Employment Opportunity and Anti-Discrimination Policy
- EDIBJ Policy