



Monash University
Medical Postgraduate Society
Class of 1974

Newsletter

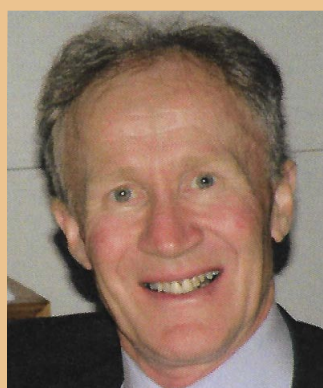


August 2026

MUMPS 1974 committee



Peter Dwyer, President



Peter McLaughlin, Treasurer



John Mackenzie, IT



Jane Fyfield, Consultant

Editorial

John Mackenzie, Committee IT

Welcome to the August 2026 edition of the newsletter.

In this issue, the much anticipated Registration for the Reunion is now open, and up-to-date information released.

Also, a recent Campus Tour highlights the extraordinary growth that has taken place at the Clayton Campus since our student days back in 1969-71.

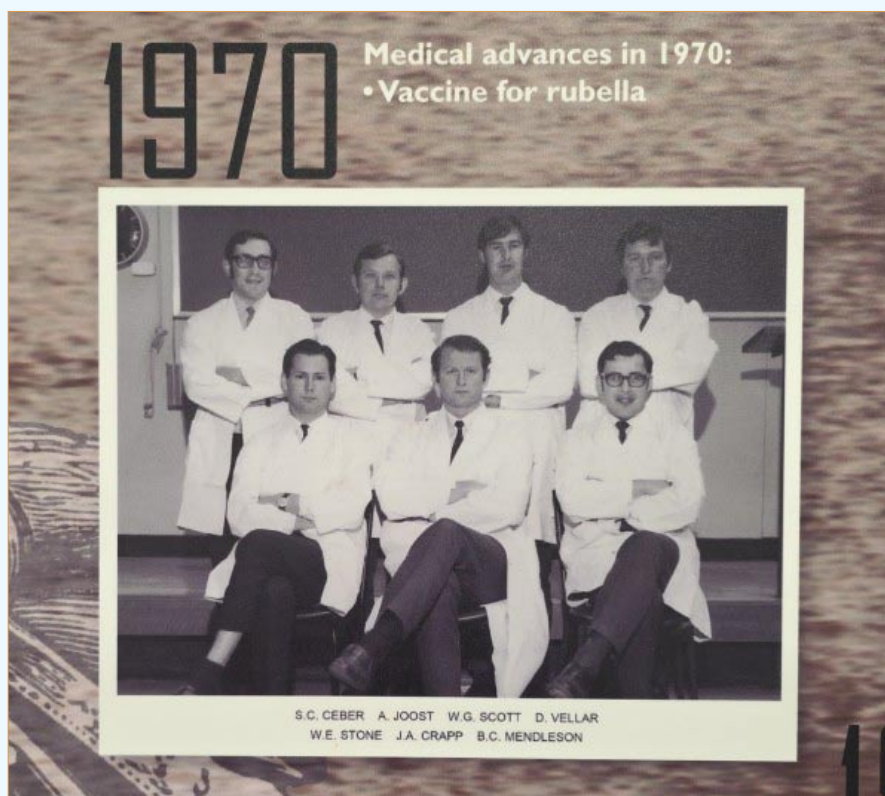
Finally, there is an article on the different methods that are being used to log in to website portals - methods which have been changing and can be confusing. The full version of the article is in the Tech Talk section of the website blog at:

<https://monash-med74.dyndns.org/blog/index.php/category/tech-talk/>

Enjoy.



Campus Tour Highlights



Recently I had a guided tour of the Clayton Campus. The staggering growth and development portrays what can be achieved with brilliant architecture and modern technology.

See the full report of my Campus Tour on the blog here:

<https://monash-med74.dyndns.org/blog/index.php/category/news/>



Reunion: Registration now open



The Reunion on **Friday 19th March, 2027** is fast approaching and registration is now open.

Get all the details and register your interest using the Online Registration Form, here:

https://monash-med74.dyndns.org/reunion_2027.html

Accommodation

Those requiring accommodation may wish to check out and possibly make arrangements at Quest Notting Hill, located on the north side of the Clayton Campus within 1.4 km of the Monash Club.

Quest has 100 serviced apartments with kitchen and laundry facilities, secure parking, on-site gym, BBQ, business lounge, and an airport transfer service, see:

<https://www.questapartments.com.au/properties/vic/notting-hill/quest-notting-hill>

Golf

The options for golf will be announced nearer the time. At this stage, please let us know on the Registration Form if you are interested in playing golf, whether you are a member of a golf club, and if your club has reciprocal arrangements with a Melbourne golf club.

Cost, invoice and payment

The cost of the reunion is expected to be about **\$125** per person (all inclusive). An invoice will be sent later in the year, which can be paid by online Electronic Funds Transfer.

We look forward to seeing you.

Date

Friday 19th March, 2027

Venues & Schedule

1. Monash University, Clayton
10:00 Start arriving/ morning tea
10:30 1st Campus Tour
11:00 2nd Tour
2. Metropolitan Golf Club
12:00 Canapés
13:00 Banquet lunch
16:00 Close

Login Confusion

For many years, logging in to websites has relied on a combination of username or email address, and password.

This system is still widely used today, however passwords have weaknesses: people often reuse the same password on multiple websites, weak passwords can be guessed, and passwords can be stolen in data breaches or scams.

Because of these inherent weaknesses, many organisations are now adding extra layers of security to log in ...

2FA and Authenticator apps

Websites are increasingly using two-factor authentication (2FA) to improve security - after entering a password, the website will send a temporary security code by text message (SMS) or email. The user then enters this code to complete the login process.

This approach still has some weaknesses - text messages can sometimes be intercepted or redirected, email accounts may themselves be compromised, codes can be delayed or fail to arrive, and scammers may trick users into revealing codes.

Therefore, many organisations (such as the AHPRA website) are moving towards the use of authenticator apps instead, see AHPRA login video here:

<https://www.ahpra.gov.au/Support/Ahpra-portal-help-centre/How-to-renew.aspx>

Authenticator apps generate security codes directly on your phone without relying on text messages or email delivery. These codes change automatically every 30 seconds.

Common authenticator apps can be downloaded and installed on your phone from your favourite app store – iPhone app store, android Google Play Store, etc. Most websites do not require a specific authenticator app – any of the following will usually work:

Google Authenticator, Microsoft Authenticator, Aegis Authenticator, Proton Authenticator, etc.

So to log into a website that requires 2FA via an authenticator app, you:

- enter your username (email) and password,
- open the authenticator app on your phone, then
- type the six-digit code shown in the phone app back into the browser screen.

Even if somebody learns your password, they still cannot log in without access to your phone and the current code. This is why authenticator apps are increasingly used for: email accounts, banking, workplace systems, cloud services, social media accounts, etc.

The emerging use of passkeys

Passkeys are a newer technology designed to eventually replace passwords. Instead of typing a password, your device securely confirms your identity using fingerprint, face recognition, device PIN, or another secure unlock method to login.

Passkeys are generally easier to use and more resistant to phishing scams than traditional passwords. However, choices are required when creating a passkey, such as where to save the passkey - to a password manager, or to the device itself, or even to a special USB hardware security key? These options are explained in the full version of this article on the website blog at <https://monash-med74.dyndns.org/blog/index.php/2026/06/12/login-confusion/>

A period of transition

At the moment, the internet is in transition: passwords are still widely used, 2FA and authenticator apps are increasingly common, and passkeys are being introduced whilst the technology is fast evolving. Understanding these processes helps clear up confusion.

