MARIST COLLEGE
ASHGROVE

What does 'access' mean?

'Access' means that some of the data stored on the College's servers was viewed by the hackers.

Please see the following question to find out what type of data was breached.

What type of data is involved?

The personal data that was breached is extremely limited and the current evidence from our specialists indicates the breach is limited to one drive only. There is no evidence that any financial details, HR details and/or driver's licence details have been breached.

How do I know if my data has been breached?

Our forensic IT and Cybersecurity experts are compiling a list of individuals who have had their data breached.

We will reach out directly to each particular individual whose data has been accessed.

Do I need to change my driver's licence details?

No. The investigations performed by our forensic IT and cybersecurity experts confirm there is no evidence that driver licence details have been breached. However, if you are still concerned, we refer you to the documents and procedures set out in our prior letter dated **15 October 2022.**

Do I need to get a new passport?

If you are not contacted directly by the College in relation to your passport details, you do not need to change, cancel or replace your passport.

We will provide further information directly to those individuals who have been affected.

Is my superannuation impacted?

No. There is no evidence that superannuation details have been breached. As a safeguard, we have written to all staff member's superannuation providers to inform them of what has occurred and to ensure that all possible precautions are taken.

How can I protect my financial identity?

If you are still concerned, IDCare recommend placing a Credit Ban, or 'freeze', on your credit file. This means Credit Reporting Agencies (CRAs) are not able to disclose any personal information from your consumer credit file unless you provide written consent for them to do so.

For more information visit IDCare's Fact Sheet (https://www.idcare.org/fact-sheets/credit-bans-australia).

Aside from this, we recommend you be on the lookout for scams, suspicious activity and transactions on your devices and accounts and change your passwords regularly.

What steps have Marist College Ashgrove taken to safeguard the data and prevent future breaches?

We have taken the following steps to date:

- Immediate shut down the breach;
- Immediately engaged cybersecurity and forensic IT experts to:
    - Safeguard and restore affected servers;
    - Investigate the data breach; and,
    - Monitor the web for any publications of the data, which is ongoing.
- Reported the breach to the Office of the Australian Information Commissioner, Australian Cyber Security Centre, Queensland Police Service, Queensland Department of Transport, and Australian Passport Office.
- Notified and regularly updated all potentially affected parents, students, and staff, all former staff, and former students (where logistically able to do so).
- We need your help in working together to keep our servers as safe as possible. To that end, we have written to you about the importance of engaging in best practice cybersecurity measures, including changing passwords often, enabling multi-factor authentication where possible and not using the same passwords online.

If you believe your data has been stolen, please notify us immediately at community@marash.qld.edu.au

The following resources and support services are also available online and we encourage you to avail yourself of them:

- IDCare Individual Support Services (https://www.idcare.org/contact/get-help)
- Educate yourself on what scams look like at the Australia Cyber Security Centre (https://www.cyber.gov.au/) or ScamWatch (https://www.scamwatch.gov.au/).

How can you be confident that no further breaches will take place?

The College engaged top-of-the-line experts to investigate this incident and we are committed to continuing to retain these experts for the foreseeable future to provide ongoing monitoring services. If there is any change to the current situation, we will provide a further update and recommendations.