MARIST COLLEGE
ASHGROVE

Data Breach Update – 3 April 2023

Those who have been following our data breach incident would know that we have had cyber experts carrying out dark web monitoring for the past 7 months.

The good news is that there is no evidence that any further information has been published on the dark web *(ie beyond what was previously publicly advised; 192 passport details which were either current or that had expired within the past three years, and some Blue Card information of some staff/ volunteers, all of which had expired by 2019 and which cannot be used as a form of primary ID in any event).*

Naturally, it is impossible (and would be irresponsible) to categorically rule out that no further information has been published on the dark web, which our dark web monitoring consultants have simply not discovered. Likewise, we accept that some cyber criminals/ threat actors are careful to delete evidence of their actions within a system.

With this being the case, and following our previous public update in February in which we stated that: *"Those people whose information was illegitimately exfiltrated know who they are as we sent personal letters to those people",* we want to be totally transparent with our school community. We are posting these updates on our website, out of an abundance of caution, to further publicise within what has occurred. This is so that those individuals, who we have not identified through our thorough cyber investigations as being directly impacted, are also fully aware of the situation that has occurred and have the opportunity to take precautionary steps should they feel that necessary, or are in any way concerned.

To this end, we would remind you of the lengths the College took to inform as many members of our school community as reasonably possible of what had occurred (including a large number of former staff, parents and students).

Information you may find useful:

The Office of the Australian Information Commissioner has some useful resources on its website which we would like to bring your attention to:

- Respond to a data breach notification
- Identity fraud.

Steps you can take to safeguard your cybersecurity

In our February update, posted on our website, we outlined some suggested steps to safeguard your cybersecurity and we take the opportunity to reiterate those steps once again:

- Change passwords to your various online accounts and enable two factor authentication if this is available and not already a requirement for those accounts.

- If you are contacted by anyone posing as someone working on our data breach, please ignore them, do not engage with them, **do not** open any emails professing to be about the data breach that are not from Marist College, and **do not** click on any links from any unknown entities. Please advise the College if you are contacted so that we can take further action.

- If you see/ experience signs that your identity has been compromised, we recommend you contact the government's IDCARE service which provides support services to individuals. IDCARE can be contacted at https://www.idcare.org/support-services/individual-support-services or by phoning toll free in Australia on 1800 595 160.

- If you are someone who was notified by us that your Blue Card information was accessed, apply for a replacement Blue Card via the following website (indeed even if you were not notified, and you know we had your Blue Card information, you may choose to apply for a new card: https://www.qld.gov.au/law/laws-regulated-industries-and-accountability/queensland-laws-and-regulations/regulated-industries-and-licensing/blue-card/existing/replace-lost-card

Marist Ashgrove remains committed to supporting any member of our school community in any way we can. We look forward to taking the lessons we have learnt from this experience and moving forward with our School community in 2023 and beyond.

Correction

In our February update, we stated that a threat actor encrypted certain servers on 19 September 2022, however it was in fact 18 September 2022.