MARIST COLLEGE
ASHGROVE

Update on data breach incident as communicating to impacted individuals – 22 February 2023

Last year, during the Term 3 break, Marist College Ashgrove fell victim to a cyber-attack. We take the protection of data and personal information very seriously and are deeply regretful this happened. We provide this post in the interests of transparency and an update on the matter.

In the hours after we discovered the breach, we took swift and decisive action to ensure we had a best-practice approach to guide our actions without delay. We engaged an independent cyber incident response team to work closely with us. That team included, but was not limited to, cybersecurity and forensic IT experts. This ensured all initial critical steps were taken as quickly as possible, aligned to cybercrime incidents such as these. It meant we were able to restore and safeguard our IT environment quickly, which was vital to ensure school operations resumed without delay for the start of Term 4.

As you know, we kept our school community as updated as possible while our experts worked hard to better understand the nature and extent of the breach. It is important to understand that all those individuals whose personal information could be deemed to cause serious harm as a result of this unfortunate incident were notified directly last year. We contacted those individuals as soon as reasonably possible once we knew for sure that their information was implicated so as to ensure they had a chance to take personal mitigative action to protect themselves as much as possible.

What happened exactly?

1. On 4 August 2022, an illegitimate third-party gained unauthorised access to the College's IT systems. All indicators are that the perpetrator was an overseas-based cybercrime group.

2. The third-party encrypted certain servers on 19 September 2022 and left a ransom note requesting we pay them in order to decrypt the data. In line with advice and guidance (including from the Australian government) we did not give in to these demands.

3. We began restoring our systems immediately, while also engaging cybersecurity experts to commence forensic investigations.

4. Our experts discovered that some of the data was exfiltrated and published on the dark web, including 192 passport details that are either current or that had expired within the past 3 years, and some Blue Card information of several staff/ volunteers, all of which had expired in 2019 and which cannot be used as a form of primary ID.

5. Based on our experts' investigations, there is no evidence to show that any financial information, bank details, human resources details, or driver licence details have been compromised.

MARIST COLLEGE
ASHGROVE

We are confident in the cyber security findings and that no financial information has been compromised.

Steps you can take to safeguard your cybersecurity

Those people whose information was illegitimately exfiltrated know who they are as we sent personal letters to those people.

Those letters, as well as the many others that we have provided to the wider school community, contained suggested steps to take, and we reiterate those below:

- 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: 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

What have we done to boost our IT security?

The College has invested significantly into services, tools and resources to bolster our IT security. For example, we have taken the following measures:

1. Reset all passwords across our systems.
2. Installed a Fortinet firewall appliance to inspect and filter internet traffic.
3. Removal of virtual desktop systems from being directly internet accessible.
4. Engaged in regular dark web monitoring.

Following these measures, we are advised that despite further attempts to get back into our systems during the Christmas / New Year break, these were successfully thwarted.

What have we done to better protect your personal information?

The College has undertaken a number of steps already, and has set achievable targets in this regard, including:

1. With respect to those individuals with affected passports, we have reimbursed any replacement fees on application.
2. Deleting old personal data from our systems that does not need to be there.
3. Creation of a Data Retention Focus Group tasked with:
    a. Reviewing and updating the College's Records Retention Schedule; and
    b. Refining our business processes when it comes to collecting data.
4. Working towards the assessment and redaction of all existing online and hard copy records by the end of 2024.

We're sorry

Again, we unreservedly apologise to our school community (and beyond) that this has occurred. We remain committed to assisting anyone who has been personally impacted in any way we can.