Notice of Data Breach with Blackbaud

Dear MA Families and Community Partners,

We are writing to let you know about a data security incident that may have involved your personal information through our Blackbaud database. Montessori Academy of London takes the protection and proper use of your information very seriously. We are therefore contacting you to explain the incident.

Quick Overview of Incident: A copy of a backup file of our database was taken by a cybercriminal through a ransomware attack on Blackbaud's hosting environment. The backup file does not have any credit card, banking information, usernames or passwords. It does have names, addresses, student birthdates and billing transaction amounts, however this was all in an encrypted file. To put it simply: it would be similar to taking a sealed box of photocopies of this information, the criminal getting paid, the box getting destroyed while still sealed, and therefore no information was accessed.

Further details of this incident are below. This has impacted numerous organizations globally; you may have also received a notification from some of them, such as universities or other large non-profits.

What Happened
We were recently notified by Blackbaud, one of our third-party service providers, of a security incident. At this time, we understand they discovered and stopped a ransomware attack. After discovering the attack, the service provider's Cyber Security team, together with independent forensics experts and law enforcement, successfully prevented the cybercriminal from blocking their system access and fully encrypting files; and ultimately expelled them from their system. Prior to locking the cybercriminal out, the cybercriminal removed a copy of our backup file containing your personal information. This occurred at some point beginning on February 7, 2020 and could have been in there intermittently until May 20, 2020.

What Information Was Involved
It is important to note that the cybercriminal did not access your credit card information, bank account information, username or password. The MA Parent Portal was not involved in the incident. However, we have determined that the file removed may have contained your contact information, demographic information, student birthdates and a history of your relationship with our organization, such as donation dates and amounts.

Because protecting customers' data is their top priority, Blackbaud paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed.

Based on the nature of the incident, their research, and FBI investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly.

What We Are Doing
We are notifying you so that you are aware of the incident and what is being done to further protect your information. Ensuring the safety of your data is of the utmost importance to us. As part of their ongoing efforts to help prevent something like this from happening in the future, Blackbaud has already implemented several changes that will protect your data from any subsequent incidents.

First, Blackbaud's teams were able to quickly identify the vulnerability associated with this incident, including the tactics used by the cybercriminal, and took swift action to fix it. We have confirmed through testing by multiple third parties, including the appropriate platform vendors, that the fix withstands all known attack tactics. Additionally, they are

accelerating efforts to further harden their environment through enhancements to access management, network segmentation, deployment of additional endpoint and network-based platforms.

In addition to notifying all affected parties directly, we have taken the following steps:

- We have informed the Information and Privacy Commissioner and will continue to work closely with their office.
- We are working closely with Blackbaud to understand why this happened and what actions they are taking to increase their security.

What You Can Do
There are no further actions required of you at this time, but out of an abundance of caution we recommend that you report any suspicious credit card activity or any suspected identity theft to your local law enforcement agency.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any further questions or concerns regarding this matter, please do not hesitate to contact us.

Sincerely,

Tina Sartori
Executive Director