Saint Cecilia's
Church of England School

"Glorifying God through outstanding, enjoyable education"

To Parents/Carers

18th April 2024

Dear Parent/Carer,

Update on IT Network Shutdown

On 5th April 2024, during the Easter holidays, Saint Cecilia's was the target of an organised ransomware attack, which affected our server and central Management Information System. The School took immediate action and is liaising with the Information Commissioner's Office ('ICO') and the National Cyber Security Centre, as well as the police and cyber security specialists, to investigate this incident.

As a number of public sector organisations have recently experienced, the criminal attack was sophisticated, access was achieved, and data was unfortunately stolen from our network.

As soon as we became aware of the attack, measures were put in place to contain and remove the malicious software and restore our systems. The forensic analysis of our network is being conducted by third-party cyber security specialists who are investigating the circumstances and impact of the incident.

We informed our community this week that we were aware of a number of documents that had been obtained by the attackers. Our external cyber security specialists have determined and confirmed to us that the perpetrators have unfortunately published sensitive personal data relating to some individuals on the so-called "dark web".

We know this will cause concern to members of our community and we are very sorry for this. Pastoral support is available to pupils and students from their mentor, Year Leader and the school Chaplain.

Our priority is to resolve this issue and provide updates as soon as we are able to, once the process of collating and categorising the data has been completed by the external teams who are supporting us. This process should allow us to understand more fully who has been affected and what data is involved. We are focusing all available resources to achieve this. We are also continuing to work with the police, the National Cyber Security Centre, Wandsworth Council and the ICO in response to this development.

While there is no evidence that passwords have been stolen, in line with good security practice, our school community and anyone with a link to Saint Cecilia's are advised to change their passwords for any online accounts they may have, for example, relating to emails, apps and websites. Please also be particularly vigilant for suspicious-looking or unsolicited emails or other activity. Parents and carers are asked to support their child to update their passwords on their personal devices. All pupils and students are being issued with new logins for their school devices.

Individuals may find the following information from the National Cyber Security Centre helpful:

- Phishing attacks - dealing with suspicious emails
- Cyber Aware - advice on how to stay secure online
- Data Breaches - guidance for individuals and families
- Cyber Security Small Business Guide

Saint Cecilia's takes the protection of its data very seriously. Our IT team is working with a specialist cyber security firm and all relevant authorities to restore full access to our IT systems for our staff, pupils and students as soon as possible.

The School will issue further updates as necessary.

- Ends -