ST STITHIANS COLLEGE

40 Peter Place | Lyme Park | Sandton | 2191
Private Bag 2 | Randburg | 2125 | South Africa
+27 11 577 6000
www.stithian.com

Notification of security compromise

St Stithians College Endowment Fund Trust ("**St Stithians**" / "**our**" / "**we**" / "**us**") wishes to provide further information to its community in respect of the information security compromise detected on 11 July 2023 ("**the incident**"), in compliance with section 22 of the Protection of Personal Information Act, 2013 (POPIA).

St Stithians is not aware of any personal information that has been published or misused as a result of the incident. However, we have taken the necessary measures to determine the scope of the compromise and to restore the integrity of our IT environment. Our efforts have been supported by a team of external legal and forensic experts.

We are providing this information relating to the incident and the actions taken by St Stithians to mitigate any possible adverse effects.

Overview of the incident

St Stithians became aware that its IT environment was unlawfully accessed by an unknown and unauthorised third party on or about 11 July 2023. As a result of this, certain servers and drives within St Stithians' IT environment were accessed and data was encrypted using a software encryption application.

A digital forensic investigation commenced immediately with the assistance of external specialists. This investigation is ongoing to determine the scope and impact of the incident. However, there is presently no evidence of the removal or exfiltration of data from St Stithians' IT environment.

Secure and up-to-date backups of the affected servers and drives were already in place, and we have restored the encrypted data from these backups with minimal disruption to our operations.

What we have done

St Stithians takes the confidentiality, privacy and security of data and personal information in its care very seriously. We have acted promptly, with the assistance of external IT and legal specialists, to investigate and resolve the incident as well as to notify our community and to report the incident to the Information Regulator. St Stithians has obtained specialist legal advice and will continue to take the necessary steps to comply with its legal obligations in relation to the incident.

We have put in place measures to monitor for the publication of any information relating to St Stithians and its related entities on the internet and the dark web. To date, there is no indication of the publication or misuse of any personal information in relation to the incident.

Security safeguards are already in place to protect data and personal information under our control. We have also deployed additional IT security measures including resetting account passwords across our enterprise and implementing real-time scanning of our ICT system.

Possible consequences to data subjects

The full extent of the incident and any impacted personal information is presently unclear, but investigations into this are ongoing.

If personal information was contained in the impacted data, such personal information may be used to attempt fraud or further security compromises, such as social engineering/impersonation attempts, phishing attacks and/or email compromises.

We encourage you, in accordance with best practice, to maintain these security measures:

- Do not disclose personal information such as passwords and PINs when asked to do so by anyone via email, phone, text messages or fax.

- Change your passwords regularly, using passwords with length and complexity, and never share these with anyone else.

- Verify all requests for personal information and only disclose it when there is a legitimate reason to do so.

- Perform regular anti-virus and malware scans on your personal computer and mobile device, using software that is up to date.

- Do not click on any suspicious links.

For more information

We remain committed to safeguarding data and personal information in our care.

If you have any questions or concerns, please write to us at rector@stithian.com