NT NEWQUAY TRETHERRAS
Be Inspired | Be Remarkable | Be Your Best

Trevenson Road Newquay Cornwall TR7 3BH
Tel: 01637 872080 enquiries@tretherras.net
www.tretherras.net

Headteacher: Mrs Samantha Fairbairn B.A.(Hons), NPQEL
Deputy Headteacher: Ms Sarah Goswell B.Ed (Hons)

Wednesday 12th February 2020

Dear Parents / Carers,

In the early hours of Monday morning, IT systems at Tretherras suffered a significant Ransomware attack. (At the end of this letter a more detailed explanation of what Ransomware is, and how it has affected us, has been provided).

Our IT staff reacted quickly to ensure that any data which hadn't yet been encrypted was safely disconnected and powered down, and that staff were kept updated during the initial investigation.

We have reported this incident to the Action Fraud, Cyber Crime Unit and Information Commissioners Office (ICO) as a crime and data breach, and are also receiving additional IT support from our Trust colleagues at CELT.

Understandably, we have already received a number of phone calls from parents querying the status of student coursework. In that respect, while we are remaining cautious to ensure that further data doesn't become encrypted, we do have backups of all student and staff work / shared data, and we can fully restore their work from backups when our infrastructure is deemed clean and secure.

Over the last few years, Staff and Students have been increasing use of Microsoft Office 365 (e-mail, OneDrive, SharePoint, etc.), and we can confirm that data which is within that platform is unaffected.

Our IT staff will be continuing efforts over the coming days and weeks to provide replacement services/servers and restore data backups.

We will of course ensure that we update you again if the above situation changes, but should you have any additional concerns, please e-mail Mark Braham, Chief Information Officer, mbraham@celtrust.org

Yours sincerely,

S. A. Fairbairn

MRS S FAIRBAIRN
Headteacher
CELT Executive Headteacher

What is Ransomware?

Many of you may have heard the phrase 'Ransomware' mentioned in the news, following other high-profile cases (the recent attack on the NHS arguably being the most featured).

Ransomware is essentially a piece of software, like a virus, that affects either a single computer or spreads across a network to affect multiple computers, and encrypts all data. The data isn't deleted or moved away from the computer, but once encrypted it becomes inaccessible to users. A person or group responsible for a Ransomware attack will then claim that they can decrypt data to make it accessible again, if a significant fee is paid via a digital currency like Bitcoins. (Other than concerns about essentially funding organised cyber-crime, there is also no guarantee that decryption will be possible, or honoured!)

In contrast to the widely reported NHS case, all of our systems were fully patched, running the very latest versions of Operating Systems (Windows 10 / Server 2019), with constantly updated Antivirus software deployed across the site too.

Unfortunately, all of these proactive steps are only as good as the last 'known' attack where Microsoft and other vendors have the opportunity to protect their customers. In our case, it appears that the specific kind of malware we encountered was a very new variant which AV companies had not been able to analyse and issue protection from.