Fylde Coast Academy Trust
Mereside Primary Academy
Langdale Road, Blackpool
Lancashire, FY4 4RR

www.fcat.org.uk

01253 207709

19 September 2024

Dear Parent/Carer

We are writing to provide you with further information following a ransomware attack which has affected Fylde Coast Academy Trust's IT infrastructure and access to our IT systems.

On 17 September, we became aware that the trust's IT infrastructure had been compromised. Within hours of becoming aware of the issue, we engaged a cyber security response team to investigate the issues with our IT system and help us restore access to our systems. This investigation is still underway, but we can now confirm that the trust has suffered a ransomware attack.

What does this mean?

A ransomware attack is where malicious software prevents you from using your IT infrastructure and data can be encrypted (meaning it cannot be used) and may also be stolen.

Our early investigation indicates that some limited pupil information has been accessed during the ransomware attack. This includes email addresses, passwords, details of pupil premium status and free school meal status. On its own, the information that has been accessed from our IT systems is very unlikely to pose any risk of identify fraud, identity theft or other risks associated with a cyber-attack. However, if this information is combined with other information available online then the risk of identity fraud may increase.

Please be reassured that we have no information currently to suggest that any pupil information has been published online or misused. The majority of the trust's pupil information is stored in a different server which has been unaffected by the ransomware attack. However, we are writing to you to explain the details of our investigation so that you are aware of the steps that we are taking to protect pupil information.

How will this impact pupils?

The ransomware attack means that we are unable to currently access some of our IT systems. During this time, we have reverted to non-IT based processes to meet our legal and regulatory duties and have acted quickly to mitigate the reduced functionality in classrooms with the use of mobile networks. Our focus remains in providing the highest possible care and education for pupils during this recovery. Leaders, teachers, support staff and pupils have responded very positively and with resilience. The skills and knowledge learnt during the Covid-19 pandemic have provided reassurance and confidence in dealing with this challenge.

Where communication systems have been impaired, we would ask for your patience and support until systems recover. Telephone lines have been quickly re-established, though with reduced capacity. We'd ask parents and carers to contact school only when necessary until further phone lines are reintroduced

What are we doing?

On discovering our IT systems had been compromised, the trust took immediate action to engage our cyber security response team to stop the attack, carry out an investigation and look at additional measures we can put in place to reduce the risk of any further ransomware attacks. This includes resetting all passwords across the trust and working with our cyber security response team to see if there any additional security measures we can implement to reduce the risk of an attack happening again.

What steps can you take?

There are certain steps pupils can take to protect themselves from the risk of identity fraud, including:

- Changing passwords for any accounts where the same password is used as the one used to access the trust's IT system.
- Ensure that passwords are not re-used across important accounts in the future.
- Ensure passwords are strong and unique and are not easy to guess.
- Enable two-factor authentication across all important accounts where this is available.
- Be alert for phishing emails and text messages – messages where the sender is prompting you to click links or enter your details.

Further advice on using passwords to protect your data and spotting and reporting suspicious correspondence is available from the National Cyber Security Centre.

What happens next?

We are continuing our investigations and we will keep you updated as our systems are restored. Advice and guidance will be provided to you actively as we receive it. We expect to see the restoration of key services start next week. However, full restoration of our systems will take a number of weeks to ensure the ransomware is completely removed.

The trust has a Data Protection Officer (DPO) to advise us on our obligations under data protection law. The trust's DPO is Peter Montgomery. If you have any concerns relating to data protection, you can contact our DPO by emailing dpo@fcat.org.uk.

We would like to take this opportunity to thank you for your ongoing support and resilience as we pull together to meet this challenge.

Yours faithfully

Dean Logan
CEO