Poole High School
VALUED • INSPIRED • EMPOWERED

12 October 2020

Dear parents, carers, guardian

Re. WisePay cyber-attack last week

We were notified last week that WisePay had suffered a cyber-attack but were given an assurance that our school had not been affected. We were also informed by WisePay that they had instigated a forced password reset on all accounts. Given the perceived absence of any threat, we sent out reset details as a routine procedure, not wishing to cause any undue alarm.

On Friday we were given contradictory information about 'disclosure risk' – this time informing us that some parents' personal details had been compromised. We took steps to notify these parents straight away. In hindsight we should have notified all parents and not just those we had been told had been affected. I apologise for this and the concern this caused over the weekend.

I am in continuous contact with WisePay about this situation. They again have given their assurance that the matter has been resolved and the website is safe to use. However, I have since contacted our GDPR Office, Handsam regarding this matter to seek external assurance. In the meantime, we are requesting a full explanation as to why we were given conflicting messages. Had the school known on Wednesday of the slightest level of threat, we could have communicated with all parents instantly by e-message.

If you have any further concerns, please feel free to contact them directly if you so choose: Richard Grazier, Managing Director, richardg@communitybrands.uk. A notice as attached is from WisePay.

Yours sincerely

Mr D Newman
Director of Finance and Operations
Poole High School

School Notice (not impacted)

We value the privacy of your information, which is why we are writing promptly to let you know about a data security incident that affected our payment platform provider, WisePay.

At some point around 2 October 2020, we understand that a cyberattack occurred in the form of a URL manipulation, meaning that the payment gateway page was redirected or controlled by a bad actor.

WisePay has engaged a computer forensics expert, and the forensic investigation is ongoing. Even though you did not attempt to make any transactions during the period in question, as best practice, we would still recommend that you are especially cautious regarding your personal financial arrangements and take prompt steps to pause or cancel the payment card you have used on our site. We also recommend you take additional precautionary steps to change passwords or login details for your bank accounts and credit cards.

WisePay has taken its website offline until the incident is remediated. It is also taking steps to implement additional security measures designed to prevent a recurrence of such an event. WisePay also has notified the UK's Information Commissioner and law enforcement to ensure the incident is properly addressed.

Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for additional steps you can take to protect your information.

Given that there are several investigations into this incident, including potentially by law enforcement, WisePay requests that you keep it confidential. For further information and assistance, please contact me.

Richard Grazier
Managing Director
richardg@communitybrands.uk

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

1. **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**
   As a precautionary measure, we recommend that you remain vigilant by reviewing your financial account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities.

2. **Copy of Credit Report**
   You may obtain a free copy (30-day free trial) of your credit report from the major credit reporting agencies by visiting:

   Experian: http://www.experian.co.uk/
   Equifax: https://www.equifax.co.uk/
   TransUnion: https://www.transunion.co.uk/consumer-solutions

3. **Fraud Alert**
   You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the credit reporting agencies identified above (as applicable).

4. **Security Freeze**
   You may be able to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency.

5. **Emails**
   Check if your email has been misused on www.haveibeenpwned.com

ONLINE
www.wisepay-software.com

CALL
0845 899 0011

Wise Pay Ltd is registered in England and Wales
Registered Office: 2 Darker Street Leicester Leicestershire LE1 4SL England
Company Reg No: 03274469 Vat No: 689397355