



# ABBOT'S LEA SCHOOL

Headteacher: Mrs Ania Hildrey, FCCT, B.Ed(Hons), M.Ed, NPQH, NPQEL



10 January 2025

Dear Families

## Re: Cyber incident at Abbot's Lea School

I am writing to inform you that the school has been subject to a cyber incident which has caused disruption to our IT services today.

We have worked with the key staff and our external IT provider to swiftly implement contingency plans to ensure minimal disruption whilst we get our system back to its normal function.

The school is taking this cyber incident extremely seriously and we are co-operating with several partner agencies, including Merseyside Police and Action Fraud to investigate this incident.

Whilst unauthorised access to school systems has taken place, we cannot be certain at this point as to whether any data on our school system has been compromised, however, to protect our stakeholders as best we can, we are working on the basis that it has, and therefore we have reported the incident to the Information Commissioner's Office (ICO).

Meanwhile, I attach to this letter some useful information passed on to me by the Merseyside Police.

I also politely ask that, should any member of the school community receive any contact – via social media, email, call or other means - from a suspicious source possibly related to this cyber incident, that they do not engage with it, but instead report it to the Merseyside Police as a matter of urgency.

We will update you once we have further information and can assure you that we are doing everything possible, together with our partners, to minimise disruption and any potential data loss.

On behalf of the school, I apologise for any inconvenience or distress potentially caused by this cyber-incident.

Yours sincerely

Mrs A Hildrey  
Headteacher

## **Information from The Cyber Dependent Crime Unit of Merseyside Police**

The Cyber Dependent Crime Unit of Merseyside Police have provided the following useful information regarding cyber security, in response to the incident at the school:

Merseyside Police are aware of a Cyber Incident at Abbot's Lea School.

We are actively working with the School, as well as Law Enforcement Partners to investigate this incident, and we are closely monitoring the situation.

In response to this incident, we have collated the following information for your reference regarding online safety.

All website links are sourced from legitimate cyber safety enforcement agencies and are provided for your own reading and also sharing to colleagues, family and friends.

Any suspicious 'phishing' or scam emails you may receive, can be forwarded to [report@phishing.gov.uk](mailto:report@phishing.gov.uk)

At present there is a wave of Scam texts being sent supposedly from genuine organisations, often referring to 'a refund', 'missed delivery' etc. These text messages can be forwarded free of charge to the number **7726**. For more guidance:

[Coronavirus scam calls and texts - Ofcom](#)

**We have included some links that may assist you regarding your safety online:**

### **PROTECT ADVICE**

Please find some useful links below which is national guidance from NCSC on Cyber Protection Tips, advice and guidance, these are great free resources and worthy of a look through the webpages.

<https://www.ncsc.gov.uk/cyberaware>

<https://www.ncsc.gov.uk/section/information-for/individuals-families>

<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>

Another great webpage which you may wish to look at is the below – **Have I been pwned** – This allows you to put in your email address and let you see if any of your Emails or Passwords have been compromised in the past, this also allows you to check your passwords and identify if they have been breached.

<https://haveibeenpwned.com/>

If you receive suspicious Emails that you believe are phishing emails I would suggest that you report the email you received to the NCSC suspicious email reporting service (SERS) which you can find the link below. This will allow us to build up the intelligence picture and prevent this from happening to anyone else:

<https://www.ncsc.gov.uk/information/report-suspicious-emails>

The below link from the National Cyber Security Centre details password managers:

<https://www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers>

This site has step by step guides on how to enable 'multi factor authentication'. It is a security feature on various sites that you may use to make them more secure:

<https://docs.microsoft.com/en-GB/azure/active-directory/user-help/user-help-auth-app-overview>

Here is information on 2FA security for both *for both 'Apple' and 'Google'* and an application setup site:

APPLE USER - <https://support.apple.com/en-gb/HT204915>

GOOGLE USER - <https://www.google.com/landing/2step/>

<https://www.microsoft.com/en-gb/account/authenticator>

## **SOCIAL MEDIA APPLICATIONS GUIDANCE**

Snapchat account 'hacked' guidance:

<https://support.snapchat.com/en-GB/a/hacked-howto>

Facebook account 'hacked' guidance:

[https://www.facebook.com/help/1216349518398524?helpref=faq\\_content](https://www.facebook.com/help/1216349518398524?helpref=faq_content)  
<https://www.facebook.com/hacked>

Instagram account 'hacked' guidance:

[https://help.instagram.com/1068717813216421/?helpref=hc\\_fnav&bc\[0\]=Instagram%20Help&bc\[1\]=Troubleshooting%20and%20Login%20Help](https://help.instagram.com/1068717813216421/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Troubleshooting%20and%20Login%20Help)

## **INSTRUCTIONAL VIDEOS**

Below are several links to some YouTube videos which focus on topics such as 'Secure Wi-Fi', 'Online Identity', 'Cyber aware' :

<https://www.youtube.com/watch?v=FAVMH3dqbLo&list=PL5gcFbG9ghq5EstDSeMUow2N3nSn36wxz&index=8>

<https://www.youtube.com/watch?v=kO8->

[Yzv8rUE&list=PL5gcFbG9ghq5EstDSeMUow2N3nSn36wxz&index=7](https://www.youtube.com/watch?v=kO8-Yzv8rUE&list=PL5gcFbG9ghq5EstDSeMUow2N3nSn36wxz&index=7)

<https://vimeo.com/staffspolice/cyber-aware>

## **SEXTORTION ADVICE AND REFERENCE**

Below are several link to outside agencies which provide advice and support to victims:

[Sextortion \(webcam blackmail\) - National Crime Agency](#)

[Sextortion and webcam blackmail advice | Revenge Porn Helpline](#)

[Sextortion – Guide and Resources - Safeguarding Hub](#)