Data Protection Training Case Studies

6 June 2024

Case Study 1

Background

The parent of a former pupil, Phillip Billing, emails a PE teacher the following.

Sent 20 February 2023

We request all of the information held on Phillip. In particular, regarding the incident which led to his suspension. I have spoken to Phillip and he consents to us making this request on his behalf. Please confirm receipt of this.

Phillip joined the School in September 2015.

One of the incidents that led to his suspension involved changing the detention list on the teacher's computer whilst the teacher was attending another student.

1. What steps should you take to deal with this request?
2. Assuming that you progress to preparing the documents below for disclosure - what should be disclosed? Which exemptions are relevant to withhold personal data?

Document 1

An archived electronic detention note from December 2016 that reads:

Student: Phillip

Reason: Constantly talking back and disrupting the class.

Teacher: Rich Smith

Document 2

Email dated: 12 January 2020

Hi Jonny

I've just caught Phillip Billing selling sweets that he bought from the local corner shop. I've warned him about this before and I think firmer action is needed.

If you are going to call his parents, please can you also talk to them about Elsa. I'm concerned that she isn't paying attention or contributing in class. Please can you ask if they have noticed anything at home?

I'll come and see you later.

Rich

Document 3

Email dated: 16 May 2022

Hi Tom

I spoke with Clara, she is happy with what we discussed and will take part in the hockey team.

Phil scored another great try on the weekend, he really could be something special.

Also, I've got a spare ticket to the rugby on Saturday, if you want to come?

Joe

Document 4

Email dated 2 February 2023

Hi Julie

I have a sensitive issue to speak to you about.

Grace Fletcher came to speak to me earlier about Phillip Billing.

She told me about some text messages that Phillip Billing sent to her. I'm not sure if there is too much in these messages in particular, but I've noticed an increase in messaging trolls and an assembly highlighting that this isn't acceptable would be beneficial.

Can we discuss later please?

Thanks

Ellie

Document 5

Email dated: 28 February 2023

Hi Sofia

I saw PB for the first time since his suspension. He seems to be doing well considering the circumstances.

Apparently his parents have now made a subject access request. Some parents just can't accept that their children aren't perfect little angels!

Joe

Case study 2

A school wishes to use an app to generate a personalised learning plan for each student. For each subject area, the school inputs material produced by each student, such as coursework and mock exam answers. In addition, each subject teacher will complete a questionnaire for each student with a mixture of multiple choice and free text answers. The data is hosted on servers provided by the app.

The app will then produce a report for each student suggesting learning areas to focus on, including trends across different subject matters. The school then produces a final report for each student, with any changes or amendments that are considered appropriate.

Can this be made compliant with data protection law? If so, what steps are needed for compliance?

Case study 3

To: bursar@abcschool.co.uk

From: roberttuck@abcschool.co.uk

CC: headofIT@abschool.co.uk

Subject: Spectacular data breach! ☹

Date: 13 August 2024

Dear Bursar

Welcome back, I hope your holiday went well.

I'm afraid to say that we had a data breach whilst you were away. My email below outlines what happened. I am also copying in Tim in his capacity as head of IT in case he has anything to add. If you think we need to do anything else, let me know.

- We found out last week (Monday 5 August) that our systems had been compromised following the discovery of malware on the network. Tim's investigation found that the malware was likely using our computing resource to carry out a "denial of service" attack on a third party. As such, it did not appear that the intention behind the attack was to access any of the personal data held on our network. We successfully removed the malware from our systems, ran a system wide anti-virus scan, and everything seemed to be back to normal.
- The next day, Tuesday, HR found that it could not access our HR database. On further investigation on Wednesday, we found that the entire HR dataset had been encrypted. On Thursday, we found a text file containing a demand for a payment of 1 bitcoin to decrypt the data. To cut a long story short we agreed to pay this following a meeting of the senior management team. The payment was made late on Thursday (8 August) but as of yet the data remains encrypted and the attacker has not responded to our further emails.
- As you know, we have an off-site backup of our data to cover for eventualities such as this. However, the HR data was not on the back-up. We recently moved from a third party hosted HR platform to a new system that stores the data locally at the school. It appears that we didn't think to include the HR data on the regular backup following the switch.
- Tim and his team have been working really hard over the weekend to identify what went wrong, I'll leave it to him to update you on this point but he suspects a member of staff falling victim to a phishing email (despite all the training and policies).
- In terms of what we've done:
    - We notified the ICO yesterday afternoon.
    - We have informed staff. We wanted to hold off for as long as possible but this was proving to be difficult. Staff were reporting from last Tuesday that they were unable to login and book holidays or submit expenses claims. We felt we had no choice but to inform staff yesterday afternoon as they'd pretty much worked out what had happened and were getting very anxious. We've put all the usual stuff in the communication that they don't need to worry etc.

Give me a shout if you think we need to do anything else but it looks like we've got it under control!

Bob