June Data Protection Newsletter

20th June 2022

(5 Articles)

The aim of this newsletter is to highlight some items which the Data Protection team have noticed schools have been or may soon be encountering.

1. Cyber Security

Recent analysis has shown that the summer months often bring an **increase** in **attempted cyber-attack**s aimed at schools, potentially due to concentrating on tasks which involve an increase in communication with third parties such as exam boards, local authorities, new schools, and job references.

Therefore, we thought it would be a great time to remind everyone of some potential cyber attack and how to prevent them.

Potential Cyber Attacks

External

- **Rogue Phone Calls:** e.g., a phone call from someone pretending to be from the cleaning organisation and **asking** for their **bank account details** to be **changed**.
- **Rogue Emails:** e.g., a disguised address pretending to be an auditor **asking for contact details of parents**. They then email the parents asking to pay money for a school trip.
- **Obtaining Email Login details**: e.g., asking someone to **input their details via a hyperlink or web portal**, then taking control of the email account to send further **phishing e**mails or inserting a message into a future email exchange and asking for bank details to be changed.
- **Ransomware** e.g., asking someone to **click on a hyperlink or download an attachment** which causes **malware** to lockdown the shared drive until a payment is made.

Internal:

- **Obtaining login details via post its** e.g., **pupil** uses the login details to access the MIS and then **change academic results.**
- **Rogue Staff** e.g., member of **staff who was suspended** and facing disciplinary logging into the system remotely and **deleting CCTV footage**.
- **USB Devices:** e.g., a member of staff brings in a **USB device** from home which **contains malware** which then attacks the system when it is connected to the computer.

Strategies to minimise risk

1. **Confirm any changes** in contact or bank account details **through another medium** e.g., phone call
2. **Install** System Security **Updates immediately** when they arrive.
3. Set up **Multi factor authentication** on your MIS and System.
4. **Know what staff has access to what systems** and areas and then ensure that access is changed or revoked when required. This can be tracked using a Joiner, Mover, Leaver Form (template available).
5. **Block removal storage devices** using your antivirus e.g., Sophos Intercept X.
6. Ensure staff have **strong** different **passwords for different systems** which are **periodically changed.** Staff's memories can be assisted via password managers. **Confirm** these rules in your **ICT User Agreement.**
7. **Check any links in emails** by hovering over them and not clicking on it, see if the landing page looks legitimate
8. **Reduce the information your present online**, change job descriptions for key roles e.g., Finance, IT. So, they cannot be specifically targeted

9. **Take your time** and **don't be rushed with emails** from third parties which include strict time pressures
10. **Backup your key system regularly**: and ensure that all new systems and areas are included, so you an **restore after an attack**.
11. **Test your backups**, working out how to do it, and that it is working/can be used.
12. **Physically protecting the server rack** in a lockable area so it can't be accessed.
13. When **system updates** occur, ensure that they have **not turned off other auto update** functions e, g, antivirus
14. **Change Default passwords** such as the WiFi

2. Disaster Recovery Plan

Almost as if the DfE were clued into the fact Cyber Attacks may be on the rise, they have **recently** updated their guidance on **Disaster Recovery Plans**.
"What is a Disaster Recovery/Business Recovery/Incident Response Plan?" is a question that the DPOs receive relatively often, therefore we thought it would be a great idea to give a brief reminder. Please also check out the DfE guidance as well.

One can use the "**say what you see" approach** with describing what a **Disaster Recovery Plan** is. But it actually contains **hidden depths** in as much that it should be a **functional, practical and efficient guide** to how you would **deal with specific issues** and then **return the school back to normal functions**.
However, very often we see a large and unwieldy document which contains no helpful information which takes far to long to review and update.
Therefore, we recommend keeping these concepts in mind when creating it

1) What are our **key systems**? e.g., MIS, Internet, Telephones.
2) Who are our **key people**? e.g., Headteacher, School Business Manager, Premises Manager.
3) **What could go wrong** with those key systems and key people? e.g., fire, cyber-attack, illness.
4) **What do we do to get back to "normal"** after something has gone wrong? e.g., staff members step up, restore from back-ups, switch to virtual teaching, send communications.
5) **Who can assist us** with getting back to "normal"? e.g., IT, MIS Supplier, Internet supplier

In the case of a cyber attack

1) What are they key systems?
   Email Exchange, MIS, Shared Drive.
2) What could go wrong?
   You could be locked out of your systems and have data extracted.
3) What do we do to get back to normal?
   Shut down the access to the attacker, assess the damage, communicate the damage and the repercussions to the individuals effected, look to restore the system from backup.
4) Who can assist with getting back to normal?
   IT Team, MIS Supplier, DPO, SLT.

A template Disaster Recovery Plan and an Incident Response plan is available upon request.

3. Covid Test Result Retention:

Those of you with a sharp memory will remember in a previous world when school staff and students were required to test for covid twice a week and then report the results to the school. This data was then **recorded in a "test kit log and COVID-19 results register**.
As we transition away from that world then the information that was collected **will need to be periodically reviewed and securely destroyed.**
The officially **retention timeframe is (12) months** from the date of the **last entries** made by the school into them.
Therefore, we recommend that you **track down your logs** and then set a calendar reminder when the 12-month period is over, and the data can be securely destroyed.
This of course should be **recorded on your Data Destruction Log**.

David Coy david.coy@london.anglican.org.uk,
Claire Mehegan claire.mehegan@london.anglican.org
John Pearson-Hicks john.pearson-hicks@london.anglican.org
Hassan Muzammal Hassan.Muzammal@london.anglican.org

4. School Leaver Paraphernalia

After discussing such heavy topics such as Cyber Attacks, Disaster Recovery and COVID, it Is time for the DPO service to get back to what it does best, acting as the "no fun police".

We are approaching the part of the year when pupils and students are moving on to attempt adventures new.

This inevitably leads to the question "**Can we pass the pupils names/photos to create a leaver hoodie/t-shirt/yearbook?".** Which then leads to your DPO furrowing their brow and taking a deep intake of breath.

From a Data Protection perspective there is **no automatic lawful basis in place to share personal data with the PTA/PTFA/Friends of/Leavers committee**, to create an item which then **puts an individual's personal data into the world.**

Therefore, you **cannot automatically hand that data over**, as it could leave you open to the "I didn't know you were going to do that, and I didn't give you permission".

1) **Transfer** the Risk to the organisation creating the Leaver Paraphernalia and **tell them to contact parents/students** to ask if they want to take part.
2) **Seek Consent**: Actively reach out to all parents or students, explain the process, and **ask them to confirm they wish to take part**, this could be done electronically. Those who don't respond, don't take part.
3) **Use Legitimate Interest**: Actively reach out to all parents or students, explain the process and then **advise that if they don't want to take part then to contact someone**. You would first need to complete a Legitimate Interest Assessment to demonstrate there is a benefit to everyone involved.

5. Annual Reviews and Training:

With each passing day we get a little closer to **end of the academic** year. With that comes the effective **cut off point** for you to book in your **annual Data Protection Review** or to book your DPO to undertake your **legally required Data Protection training**.

- **Reviews**: We recommend that **every year** you should have a **full data protection review** where your DPO can check everything from your policies and procedures to where you are displaying data. We **don't aim to catch you out** with our reviews, the aim is to discuss any potential issues and **work with you to help** find an optimal resolution. Your DPO would then create a nice shiny report which can be shared with your governing body.
  This can be undertaken in person or virtually.
- **Training**: One of the first questions that the ICO ask whenever a Data Breach is referred to them is "when did the member of staff last have Data Protection Training". Their expectation is that this should be happening at a **minimum every two years** and if you haven't recently told someone what they should be doing how do they know better, therefore **greater blame would fall on the organisation for not properly training your staff.**
  Luckily the Grow Data Protections service **offers free Data Protection Training** as part of your package, this can be booked in for twilight or inset sessions.

Book your DPO today or potentially be disappointed tomorrow.