One West Newsletter

Welcome to the One West Newsletter.

Its been some months now since GDPR arrived and our DPO Service is proving to be very popular.

This issue focuses on Business Continuity and Cyber Security which are key aspects of our service and especially relevant at this time of year.

i-West and Audit West are part of One West which is a trading arm of Bath & North East Somerset Council.

We are now growing the range of professional consultancy services we offer and are launching our new web site. You can check it out at **www.onewest.co.uk** – we would love to know what you think.

Inside this issue:

Cyber Security

Subject Access Requests

Information security tips

In the news

Cyber Security

We are hearing more and more about the threats posed by Cyber Security. The challenge is that we have increasing reliance on IT whilst hackers and others get more sophisticated. The good news is some basic measures will go a long way to reducing the potential for an attack.

It helps to understand there are four main areas of risk for schools:

Malware and Ransomware

Malware and Ransomware are umbrella terms for anything that could have a malicious, undesirable impact usually blocking access to a computer system. Often this is until a sum of money is paid. Both can enter systems in a variety of ways.

The most common are email with malicious attachments, accessing a website that contains malicious content and connecting removable media like memory sticks to the system. Staff need to be careful in their use of IT systems in these areas.

Inappropriate use of IT resources and internet access

Inappropriate use of systems can be inadvertent or deliberate. It is a big risk which needs to be reduced.

Its essential to ensure that staff have received appropriate training, that clear policies and procedures are in place, and that the ability of staff to make changes to systems are appropriately controlled.

Denial of service

A denial of service (DoS) is a cyber-attack where someone tries to make a network resource unavailable by disrupting services of a host connected to the internet. This can prevent the organisation from being able to conduct its day to day activities which can be very serious. Firewall security in particular is essential here.

Disclosure of information

Protecting IT based information assets is critical to avoid accidental or unauthorised disclosure.

Staff need to be aware of the protocols when accessing personal information and ensure that access to the information is appropriately controlled to reduce the risk of any problems.

In the news:

- **School safety & security has been in the press a lot.**

There have been some terrible events in the USA – thankfully not repeated in British schools but still really relevant.

The DofE has launched a consultation on school safety and security guidance. This is running between the 26th November and the 18th February 2019 and will probably result in requirements on schools to address this.

The consultation web site is www.gov.uk/government/consultations/schoolsecuritydraftguidance.

- **Facebook are in the spotlight over data handling issues**

A cache of Facebook documents has been seized by MPs investigating the Cambridge Analytica data scandal.

Rarely used parliamentary powers were used to demand that the boss of software firm Six4Three handed over the details.

The Observer, which first reported the story, said the documents included data about Facebook's privacy controls.

Facebook has demanded their return.

- **The BBC has reported German children were nearly banned from sending Santa letters!**

Privacy rules in Bavaria threatened Christmas tradition. A town in Bavaria, Germany, has a Christmas tradition where children are invited to write letters to Santa Claus requesting gifts and experiences.

The letters are then put on the Christmas tree in the town's marketplace.

This year, the tradition looked like it would have to end due to rules to protect the use of data. That was avoided when the local radio station Antenne Bayern stepped in and now the tradition will go ahead with good sense prevailing!

The full story can be found on the BBC web site www.bbc.co.uk/news/topics/gdpr .

So what next?

We know this is a complex area and we will be writing more in further newsletters. In the meantime if you have any queries we would be happy to talk with you.

DPO Tips

Minimising risks around data and IT comes down to good practice. There are some key principles to adopt.

1. Protect personal data like it was your own - It's a great reminder to ensure protection

2.If you are not there to look after it, secure it! – Put data records away and out of site

3.Make sure Wi-Fi connections are secure - If they aren't others can use your internet connection.

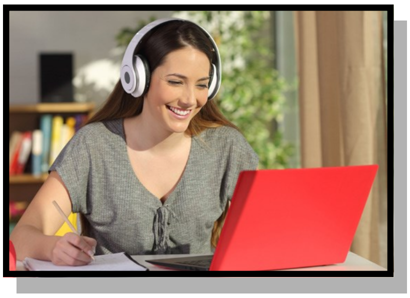
4.Don't trip up! - When returning from school trips, shred your trip pack. These contain significant sensitive data including students' health needs.

5.Only use your official email address – If you don't not only can the security of the information be compromised but if there is a subject access request it you might have to surrender your personal email account or device for scrutiny.

6.Reinforce whats required to those such as governors and peripatetic staff - these people are in school less frequently and may be less clear on good practice .

Subject Access Requests

Subject Access requests (SARS) can be tricky and some of you might not be sure what's required. Here is a guide:



The Data Protection Act 2018 gives people the right to request information that is held about them. This is known as a **Subject Access Request**.

There are some exceptions for example some safeguarding records or information provided by or related to third parties but in the main the right is there.

All types of information may have to be disclosed including handwritten notes, emails, texts and audio recordings.

Schools are receiving increasing numbers of SARS either directly or as part of complaints. When this happens both the request and complaint must be answered as separate processes.

People will often not call what they want a 'subject access request'- they just want information!

Consequently it's important that all staff can recognise an SAR and respond correctly, this is particularly relevant to frontline staff such as receptionists who are often the first point of contact for parents and members of the public

The first steps you need to take when the school receives an SAR are to:

1) Confirm the identity of the sender – for example is the email address exactly the same as on record.

2) Let the sender know that you have received their request – tell them you are dealing with it.

3) Note the date that you have received the SAR - Usually you have one calendar month to respond. However this can be extended if the request is particularly complex.

4) Locate the information that is being requested - It may be held in multiple sources, possibly with different departments.

To help further we are aiming to publish a broader guidance document soon. In the meantime we are happy to discuss any queries that you have.

Seasons greetings

We would like to take the opportunity to say all good wishes for Christmas & a happy New Year.

The staff at One West