



**Important information – please pass to
your Business Manager**

**6 weeks of advice on approaches to Cyber
Security**

Cyber Security #3



It's time to ask questions & get some assurance on Cyber Security.

The pressure on schools to make sure they have appropriate responses to Cyber Security risk is **increasing**.

It's not just about Cyber threats though – it is also absolutely about risks of **data breach** (GDPR).

It must feel like a lot to deal with, especially as this year has been so affected by our ongoing restrictions.

We are partnering schools to help.

Right now, the major agencies concerned with Cyber Security are giving some very clear messages to schools.

The **DfE** has recently corresponded to ensure schools are active in mitigating risk & the Police via their Regional Organised Crime Units (**ROCCUs**) are putting out strong messages to take great care.

Importantly, the National Cyber Security Centre (**NCSC**) is giving very clear advice especially to school **Governors** to actively assure themselves that all is in hand.

They see 8 key areas of concern that Governors should be interested in:

An understanding of the IT provider (with implicitly their measures & confidence in threat response).

An understanding of the arrangements within the school of management & coordination of IT.

Consideration of the most critical parts of the 'digital estate' & its security.

Sufficiency of back up & restoration plans.

Appropriate governance & IT policies.

Sufficiency of training in common cyber security threats.

Resilience in case of data loss or other IT access issue.

Understanding of what to do if a victim of a cyber incident.

When you get Governor interest (& our advice in any case is to get ahead of the curve & pre-empt this) it's really important to understand **one** thing.

Cyber security is **not** purely an **IT issue** – it is a **business issue**. The nature of Cyber Crime is that it does not operate purely within the IT 'bubble' at all.

In fact, we have had recent contact from schools regarding phone contact from scammers saying they are from Avon & Somerset Constabulary, trying to obtain personal data. It's pretty brazen stuff & for some, clearly worth it.

Also, very often when things go wrong, the major issue is that it is in fact a **Data breach** subject to GDPR regulations & sanctions from the ICO. So – in fact Cyber Security and Data Protection are very **closely linked**.

This offers the opportunity to address **both together** & that is where we can absolutely come in.

We already work with many schools to provide **Data Protection** & are also now providing **Cyber Security Health Checks**.

We can do this for **new** or **existing** clients – we welcome both.

Of course, where we can provide this along with Data Protection compliance, it offers an opportunity to cover both in a way that is particularly **efficient & affordable**.

We think it is difficult to match.

Interested? We are booking in appointments to discuss so let us know. We would love to talk with you.

Contact:

Steve_Debruin@bathnes.gov.uk or

Jo_Buchan@bathnes.gov.uk

Thanks & we look forward to telling you more.

The One West Business & Cyber Security team.

Watch out for our next bulletin **Cyber Security #3** – part of our **6 weeks of advice** on this extremely important topic.



Copyright © 2021 One West, All rights reserved.

Our mailing address is:

One_West@bathnes.gov.uk

Want to change how you receive these emails? Just let us know
