

 **Directorate for Children’s Services**

Buckinghamshire Council

The Gateway

Gatehouse Road

Aylesbury HP19 8FF

richard.nash@buckinghamshire.gov.uk

01296 395 000

www.buckinghamshire.gov.uk

 10 November 2021

To All Heads and Chairs of Gov.

Dear Colleagues,

**Re Cyber Attacks on Schools and Public Bodies**

I am prompted to write to you because of a growing and clear threat to us all from ‘cyber attacks’. The National Cyber Security Centre are aware of groups of individuals who proactively target schools and other public bodies in order to compromise computer systems and to steal sensitive information. Their motivation is profit through the sale of material on the ‘dark web’.

Schools are deliberately targeted by groups and are in all probability seen as a ‘soft touch’. The implications for schools that are successfully targeted are both significant and costly. Examples of the impact may include:

1. Informing the Information Commissioners Office that sensitive information has been lost.
2. Managing the communication of a data breach with pupils, staff, partners and parents.
3. Losing all of the schools systems for an unknown time period.
4. Commissioning IT expertise.
5. Significant reputational damage
6. Creating safeguarding risks for children and young people.

Any incident will attract a lot of attention that will focus on the systems that are in place to prevent malicious software attacks, whether these are up to date and whether file retention and storage policy is effective and appropriate.

It will be far less work for all of us and safer for our children, young people and their families if we can collectively and individually ensure that our systems, processes and knowledge on this issue are as strong as they can be. I strongly recommend that you carryout an urgent audit of your systems, policies, processes and knowledge of this issue across your whole staff teams.

Attached to this letter is an information sheet that provides further context on ‘cyber-attacks’, information and where to go for advice. Our advice is for you to immediately find out:

1. If your Cyber Security software and systems are up to date and that these are routinely upgraded.
2. If your staff teams are aware of this threat and are aware of the risk of opening attachments in e mails and suspicious e mail activity.
3. If you have an appropriate file destruction policy.
4. If you keep sensitive documents such as child protection reports or referrals securely and use encryption where appropriate.

I fully appreciate how busy you all are and having another task to do is not what you would wish to receive. However, the implications of getting caught out by this form of criminality is incredibly difficult and time consuming.

Yours faithfully



**Richard Nash**

**Corporate Director Children’s Services**