# Buckinghamshire Council spectacular landscapes logo

# **Ransomware**

**Cyber-Attacks on Public Organisations**

It is absolutely clear that organised gangs proactively target a whole range of organisations, including schools, in order to steal information and disrupt computer systems. This document is for your reference for you and your staff. Please share this across your school and take urgent steps to ensure you have the right level of security in place.

## What is Ransomware?

* Malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker.
* Attacks are financially driven
* They cause considerable damage in terms of potential permanent loss of data as well as loss of access to critical services for a protracted period, reputational damage and financial cost.

## How does it work?

* Ransomware takes advantage of system weaknesses such as unpatched software, poor authentication systems or the susceptibility of users to misdirection.
* Data is normally copied to the attackers as well as being encrypted on your system.
* Attacks often happen during school holidays, when there is less network traffic and the ransomware can deploy more easily without detection.

## Who is at Risk?

Public sector organisations are preferred targets, because of the sensitive and private information that is held. If a school is subject to a successful attack there is a distinct possibility that all data will be released, either publicly or on the dark web.

## What Should Schools do?

* Governors, Senior Leaders and Staff need to be aware of the threat
* Carry out regular cyber security training for all staff to ensure that they do not connect unauthorised devices to the network (such as USB keys), download unauthorised software or click on links from Phishing emails.
* Have an Incident Action Plan as part of your continuity planning
* Ensure that your IT infrastructure and all devices on it have strong anti-virus/malware software including specific elements that defend against ransomware.
* Ensure all devices connected to your network only have fully supported operating systems and software installed and that all security patches have been applied, ideally within 14 days of being released
* Ensure you are not running any end-of-life kit or operating systems that will be vulnerable to attack as there won’t be any security patches
* Ensure that a robust password policy is adhered to, making it harder for hackers to gain access. For key accounts and any remote access solution it is critical two factor authentication is used for access. Two factor authentication is a security system that requires two separate, distinct forms of identification in order to access something. The first factor is a password and the second commonly includes a text with a code sent to your smartphone, or biometrics using your fingerprint or face.
* Ensure that your curriculum and admin systems are separate.
* Consider regular penetration tests by an approved company that will identify any vulnerabilities you may have.

There is a significant amount of support at [Cyber Security for Schools - NCSC.GOV.UK](https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools)

## Minimise the impact of an attack

* Identify your data areas that may be at risk - consider the impact on a child/staff if their information, were to be made public.
* Remember the rules for personal data :
* Is it sensitive? What would be the impact if this data was released?
* Have you considered how long you store personal data? Do you have relevant disposal policies in place?
* Could you legitimately delete it? Could the information be anonymised?
* If it is archived data that has to be legally retained, does it need to be on a connected drive? School data retention information and guidance can be found [here](https://www.gov.uk/government/publications/data-protection-toolkit-for-schools).
* Review your backup procedures:
* Are you backing up the right data? –consider including Covid-19 testing information and associated data, data relating to exams and other key elements.
* Backups should be done on a regular basis.
* Backups are held fully offline and not connected to your systems or in cold storage. If they are on the network and a hacker gets in they will often target these first.
* Backups are tested appropriately – ensure they have been tested so you can restore services and recover data.

## In the event of an attack

* Do not click on any link that the ransomware provides for you.
* Switch everything off.
* Contact your IT support.

## Next steps

* Inform the **National Cyber Security Centre** - [Reporting a cyber security incident (ncsc.gov.uk)](https://report.ncsc.gov.uk/)
* Inform **Buckinghamshire Council** - **01183 589332** ask for Duty Resilience Officer to be paged, leave contact details and summary of situation
* Inform the **ICO** - [Report a breach | ICO](https://ico.org.uk/for-organisations/report-a-breach/)
* Inform the **police** via [Action Fraud](https://www.actionfraud.police.uk/)

If you would like technical support with these issues then please contact Simon Hobdell, Technical Team Leader in the Schools Technical Support Team; Simon.Hobdell@Buckinghamshire.gov.uk