CSW Resilience Team
Coventry, Solihull and Warwickshire Council's
Planning, Preparing and Responding to Emergencies

Spring Term Preparedness: Learning from a Cyber Incident and Staying Resilient

Happy New Year and welcome back!
As we begin the spring term, it's a great time to reflect on recent events and how they reinforce the importance of school preparedness across all risk areas, including cyber security and winter continuity planning.

Case Study: Cyber Attack on Higham Lane School

Over the Christmas break, Higham Lane School in Nuneaton was hit by a cyberattack, rendering its entire IT system inoperable and forcing the school to remain closed for several days while recovery work took place. Staff and students were advised not to log into any school systems until specialists had investigated and restored services. The disruption affected telephones, emails, Google Classroom, and core management systems, with reopening delayed while safe restoration continued.

This incident illustrates how cyber threats can affect operations, communications, and wellbeing, even during holiday periods. It reminds schools that preparing for digital disruptions is now as important as preparing for weather or physical emergencies.

Why Cyber Security Matters in Education

Cyber attacks on schools are common, a national cybersecurity survey found that most secondary schools have experienced breaches or attacks in recent years, with phishing and ransomware among the most frequent threats.

Schools hold large amounts of sensitive data and rely on digital systems for teaching, administration, and safeguarding. When systems fail, it can:

- Disrupt learning and communication
- Risk exposure of personal data
- Affect exam access and planning
- Place strain on families and staff.

What Schools Can Do: Practical Guidance

The National Cyber Security Centre (NCSC) offers a range of free, practical resources for schools and staff to help improve cyber resilience — from staff training to governance tools and reporting guidance.

Key steps schools may consider:

- **Ensure staff complete NCSC cyber training** — awareness is one of the strongest defences against common threats like phishing. NCSC

- **Review and test your cyber incident response plans** so everyone knows what to do if systems go offline.
- **Implement strong password policies and multi-factor authentication** where possible.
- **Regularly assess cyber risk and document mitigation actions** (e.g., through termly reviews).
- **Keep up to date with guidance and reporting procedures** via the NCSC schools pages.

Useful link:
NCSC — Cyber security for schools: https://www.ncsc.gov.uk/section/education-skills/schools

Cold Weather & Everyday Preparedness

As winter lingers, schools should also *maintain awareness of weather and infrastructure risks* that can disrupt operations.

Helpful external resources include:

- **Met Office Weather Warnings:** https://www.metoffice.gov.uk/weather/warnings-and-advice
- **Flood alerts and risk:** https://www.gov.uk/check-flooding
- **Cold weather health guidance:** https://www.gov.uk/government/collections/cold-weather-plan-for-england

A reminder to check severe weather plans, communications with families and staff, and site access arrangements now, so everyone stays safe and informed throughout the season.

Preparedness Is a Shared Responsibility

Preparedness doesn't stop at having a document , it requires awareness, dialogue, and practice. Whether it's a cyber incident, a power outage, or icy conditions, walking through "what we would do if..." helps build confidence across your team.

Thank you for your ongoing commitment to keeping our schools safe, resilient, and ready for the unexpected this term.

If you have any queries please contact the CSW Resilience Team.

Email: CSWRT@warwickshire.gov.uk