WHITWORTH COMMUNITY HIGH SCHOOL

Cyber Security Policy

Date effective from:	April 2025
Prepared by:	P Bland
Date of next review:	April 2026

Contents

Section 1: Policy Rationale

The Department for Education and the National Cyber Security Centre (NCSC) have been made aware that schools are an active target for cybercriminal gangs.

Schools can also be vulnerable to students as threat actors, and even on occasion disgruntled (ex) staff.

Reported attacks on schools include ransomware attacks and financial scams, including via spear phishing attacks, and DDoS attacks.

It is important that education professionals understand the nature of the threat and the potential for ransomware to cause considerable damage to their institutions in terms of lost data and access to critical services.

Section 2: How we will respond

What should I do if I am affected?

1. Enact your incident management plan - contact Lancashire LEA
2. Contact Action Fraud on 0300 123 2040 and press option 9.
3. Contact Network Connect on 0161 214 2020 if any action at the firewall may help to mitigate the attack.
4. Inform the North West Regional and Organised Crime Unit (NW ROCU) via cyber.protect@nwrocu.police.uk
5. Inform the Department for Education by emailing: sector.securityenquiries@education.gov.uk

The Department for Education supports the National Crime Agency's recommendations not to encourage, endorse, or condone the payment of ransom demands.

Payment of ransoms has no guarantee of restoring access or services and will likely result in repeat incidents to educational settings.

Section 3: How we will act to prevent data loss

It is vital that we continually review our existing defences and take the necessary steps to protect our networks from cyber-attacks.

Annual cybersecurity training will be given to all staff – awareness is the most cost-effective single defence against cyber attacks.

We are registered with the police Cyberalarm and NCSC MyNCSC services for monitoring and information.

Our network is externally defended by an effective and professionally maintained and supported firewall appliance.

Security patches are regularly applied to our internal systems.

Along with our defences, having the ability to restore the systems and recover data from backups is vital.

We are ensuring an effective, secure back strategy by:

- backing up all of our relevant locally held data (except for CCTV footage, which is prohibitively large) each night locally and online. This includes full virtual machine backups for all VMs for faster, more effective recovery.
- taking backups using a dedicated appliance running a hardened Linux platform saving to a dedicated online service. This forms a “nearly offline” backup which cannot be degraded without the compromise of multiple, disparate platforms.
- periodically testing restores of both individual files and full virtual machines

- using Google Drive for our online file and email platform. This ensures high levels of security and efficient file history, with Google Vault retention providing an additional route to recover any lost data.

Section 4: Roles & Responsibilities

Role	Responsibility
Updating the policy annually or in line with JCQ updates	P Bland
Ensuring all staff are trained on and are familiar with the policy	P Bland
Ensure all the right data is backed up regularly.	R Bradley
Ensuring the policy is updated and placed on the school website	L Rawstron
Ensuring Governors and Stakeholders are informed of policy	A Oliver
Ensuring backups are held in at least 3 versions, of which at least one is offsite	R Bradley
Ensuring testing and recovery of data has taken place	R Bradley
Maintaining registration with appropriate online information and monitoring services	R Bradley