Cyber Security Policy

Network configuration for cyber security

Protection against cyber attack

- We use a true cloud antivirus. This means that as long as the device has internet access they will always be up to date. This does not matter whether the device is in school or not. This antivirus updates every 15 minutes.
- We have multifactor authentication enabled for all emails. This makes it much harder for hackers to hack into the network, as it requires the hacker to have the email address, the email password and the 6-digit code from the personal mobile device.
- We run VLANs on our infrastructure, which splits up traffic on the network also making it harder for a hacker to gain personal data.
- We have disaster recovery documents and procedures that we would follow if the school were to be hacked.
- If an exam was in place and we were hacked, we would be able to join the exam laptops to a different wireless VLAN meaning that the exams can continue after 2-3 minutes of configuration on the laptops. This would block access from the exams' laptops to the school network; however, they would still have internet if needed.
- We have externally hosted firewalls meaning it is harder for a hacker to gain access to our firewall data.

Signed – Headteacher
Print Name: **Ross Whitaker**

Date: April 2024
Next review due: April 2026