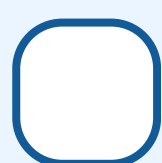


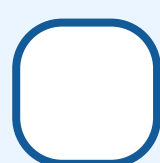


Back to school is a peak time for cyber attacks. New students, equipment, and staff accounts mean there are increased opportunities to exploit vulnerabilities. Here are some actions you can take now to set you up for the school year.

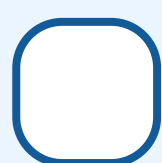
Autumn term actions



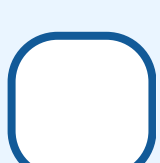
review and remove expired or dormant accounts



[register for the Early Warning Service](#), a free cyber threat alert service



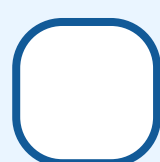
[enforce multi-factor authentication \(MFA\)](#) on all staff accounts, especially email and remote access



refresh staff training using the [NCSC cyber security training for school staff](#)



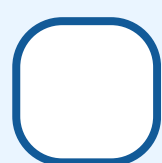
check software, security patches, and anti-phishing protections are up to date



remind staff of [strong password policies](#)

Review and update your cyber response plan

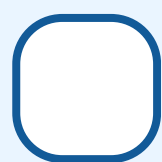
Review and update your cyber response plan at least once a year:



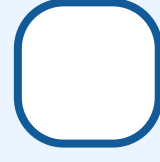
check staff roles and responsibilities are accurate



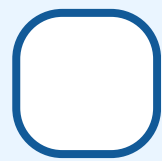
find templates and guidance on our [cyber response plan pages](#)



make sure contact details are up to date



back up and print out new copies of your plan



[follow our checklist to get your plan ready](#)

Planning ahead?

[Attacks and the school year](#) has actions for the whole year.

You can also use the [Plan technology for your school service](#) for recommendations on how to meet the DfE cyber security standards.

Find out more about keeping your school safe all year round on the Department for Education Cyber Security Hub.

A web version of this page can be found at: <https://cyber-security-hub.education.gov.uk/back-to-school>

