Department for Education

Cyber Security Guidance – March 2023

Cyber-attacks on education undermine the hard work of school leaders and are completely unacceptable. Unfortunately, cyber incidents will happen. Common attacks include hacking, phishing campaigns, distributed denial of service (DDoS), and ransomware. If any of these attacks are successful, they could cause significant disruption to your organisation. Education settings are directly responsible for their own cyber security and data protection and need to ensure they have the appropriate level of security protection procedures to safeguard their systems, staff, and learners.

Data & systems

Understanding the value of the data your school or college holds, is critical when it comes to taking steps to secure it. Mandatory GDPR regulations have highlighted the need for secure storage and protection of personal and sensitive data, but when it comes to considerations for cyber security, schools and colleges need to also ask themselves the following questions:

What data and systems are essential for the everyday running of my school or college?

What data and systems do I need to open the door on a workday morning and keep everyone safe?

What data could cause significant reputational damage if it fell into the wrong hands?

Whatever the answer is to the above questions, this is the critical data that you need to ensure is protected with user access control policies such as restricted access, strong password controls, and Multi-Factor Authentication (MFA), equally consider your access control policies in line with certain admin accounts and systems. As senior leaders, make sure that you can access and recover this data as quickly as possible following an incident. One way of doing this is to ensure that you have secure up-to-date backups so that if the worst happens and you do fall victim to a cyber-attack, you can help minimise the impact and recover from it as quickly as possible.

As exam season approaches the Department for Education is reminding schools and colleges to review their cyber security and backup policies to ensure that all critical data, including materials relating to non-exam assessment evidence, are covered within. You

may also receive information from awarding organisations about cyber security and any processes that your school or college should follow.

The Department for Education have published Cyber Security Standards for schools and colleges. Please confirm with your IT team or provider that they are following these standards.

We also recommend keeping up-to-date with the advice available on the National Cyber Security Centre's (NCSC) website. Here you will find specific guidance on backing up your data and advice on how to manage the storage of this. There is information regarding free cyber security tools as part of their Active Cyber Defence programme, including:

- Early Warning – designed to inform organisations of potential cyber-attacks against their networks as soon as possible.
- Web Check – this service checks your website for common vulnerabilities and misconfigurations
- Mail check – assesses email security compliance, helping domain owners identify, understand, and prevent abuse of their email domains.

To help with managing cyber security, here are some considerations that you should include in your cyber security planning and discuss with your IT team:

- Determine which IT systems and data are held and which of them are vital for the operating of your school or college. Communicate this to your admin & IT support teams to ensure that accurate asset and information asset registries and network diagrams are kept.
- Ensure backups of data are made and these are kept separate from the physical network, especially for the critical data you have identified. .
- Ensure the IT support team have a regime to ensure that security patches are applied to all assets and identify and report any assets which can longer be patched.
- Conduct a risk assessment to ensure that the value such obsolete assets bring outweighs the greatly increased security risks they bring.
- The benefits and risks of cloud vs on-site and migration to the cloud. The government is encouraging the move of its systems to the cloud, as cloud networks are usually more secure.
- Determine that user access control policies are fit-for-purpose. This includes limiting the access of student, staff and support accounts; preventing weak, common, default or permanent passwords being used; and enabling multi-factor authentication.
- Arrange regular training for staff on how to avoid cyber incidents (such as: NCSC's Cyber Security Training for School Staff.
- Determine the Bring-Your-Own-Device (BYOD) policy. The more open the policy, the more IT support work and infrastructure is required to set-up secure networks.
- Segment your network to slow down an attacker and potentially contain the impact to a singular segment.
- Include a response to a cyber incident in the Business Continuity and Disaster Recovery plans. This plan must be tested to ensure staff know what to do and sufficient resources are allocated. If external resources will be required, particularly a Cyber Incident Response (CIR) company, identify these.

- Confirm that IT support is using all the resources being made available to them from the NCSC & DfE. i.e Cyber security standards, Web check, Mail check, Early warning.
- Cyber insurance cover to alleviate the financial worry should an attack take place.
- Keeping up to date with the latest threat and mitigation information.

The NCSC provides guidance on developing incident response plans, items to include are:

- Key contacts – Senior management, IT, CIR company, HR and Legal teams
- Escalation criteria
- Basic flowchart process
- Basic guidance on legal or regulatory requirements i.e reporting data breaches to the ICO.

If you do fall victim to an attack or incident, you should:

1) Enact your incident response plan straight away
2) Report this to Action Fraud **(0300 1232040**)
3) Report this to NCSC
4) Inform DfE by emailing Sector.incidentreporting@education.gov.uk.

In addition:

5) If it compromises any aspect of exam or assessment delivery, report any incidents to the relevant awarding bodies.
6) If there is a suspected personal data breach, please inform the ICO either online or contact them via their helpline (0303 123 1113) within 72 hours.
7) You should also inform other organisations if you have access to their systems to prevent any unauthorised access, for example, UCAS.

If you have any questions or would like any further information or guidance, please contact the DfE Sector Cyber Security Team at sector.securityenquiries@education.gov.uk