Cyber security in schools

Cybercriminals are increasingly targeting public and private organisations, as well as private individuals.

With more people working from a variety of locations, we are encouraging all schools’ staff to follow their security procedures and change your passwords at regular intervals. Consider multi factor authentication and regular systems testing.

Review and ensure that your ICT provider and any purchased package or planned works when in-house are providing adequate levels of assurance and security which is then regularly reported to the head and governors.

Here is Ealing schools' cyber security guidance from Ealing Council's chief information security officer (CISO)

Recent cyber attack incidents

Schools hit by cyber attack and documents leaked - BBC News

Dorchester school IT system held to ransom in cyber attack - BBC News

Three-quarters of schools hit by cyberattack incidents | Tes

Recently a local school was subject to a cyber-attack which led to a significant loss of records and the need to entirely rebuild their SIMS database and school networks. The council also had to switch off access to its systems and stop information sharing until the school could be given a clean bill of health.

We suggest that along with the head that all staff, governors and students participate in regular training and an update on cyber security is reported at regular intervals to governors. A failure to do so may lead to invalidating insurance claims.

School duties

All schools have delegated duties and budgets to effectively manage ICT systems, data security and infrastructure. Schools have a range of approaches from commissioning a support provider to having an inhouse or hybrid approach.

Local Authority duties

The LA is the responsible body for maintained Schools. For voluntary aided, foundation, academy schools this is the respective trust, governing body, or faith/Diocesan board. As the LA shares and receives data from all state funded schools, the LA may seek assurance that its data and systems are protected.

For LA maintained schools, from academic year 2023, the LA will commence an assurance cycle, similar to that of health and safety.

Should schools wish to access support and services from the LA these may be considered on a traded basis.

Risk Protection Arrangement (RPA): Cover Comparison

Council insurance

Reporting incidents

In the event of a significant cyber security incident the DfE provides guidance to schools. It is also essential that schools immediately notify the relevant stakeholders below:

- Notify the LA: Suspicious@ealing.gov.uk, griffink@ealing.gov.uk and Axee@ealing.gov.uk
- Notify governors
- Notify the DfE: Sector.Incidentreporting@education.gov.uk
- Notify insurance provider
- Notify Action Fraud

Consideration should also be given for communication to staff, families and to the press.

Further guidance and information

DfE guidance - Cyber security standards for schools and colleges

Broader DfE guidance - How schools and colleges can meet IT service and digital equipment standards

The National Cyber Security Centre Practical resources to help schools improve their cyber security, including information for governing boards and senior leaders, school staff, school IT (admin teams, procurers and providers), other useful resources and advice, and how to report a school cyber incident.

The risk protection arrangement (RPA) for schools How public sector schools can join the risk protection arrangement (RPA). An alternative to commercial insurance that may save time and money.

Was this page useful?

- Yes
- Neutral
- No

Last updated: 09 Oct 2024