Cybersecurity Awareness and Training Guide

The purpose of this short guide is to provide guidance and supports to schools on how to support cybersecurity awareness and training in their schools to enable staff and students/pupils to better understand both the cybersecurity risks as well as their individual and collective responsibilities to better protect themselves and the school from cyberattacks.
The training programme needs to be consistent with other school policies such as their school Acceptable Use Policy (AUP), the School Data Protection policy and with GDPR principles.

There are two main types of cybersecurity awareness and training

School Leadership Focus:
The first focus area relates to the role and responsibility school leadership to make cybersecurity a school priority. It also relates to some of the more technical aspects of managing school systems in relation to cybersecurity. This type of training is relevant to specific teams and/or individuals in the school. Having a school cybersecurity policy in place is critical, and is a statement of intent by the school leadership team. Cybersecurity needs to be a top priority for the school leadership team, supported by the board of management (BOM), in terms of protecting school systems and school data, to reduce the risk of a cyberattack or a data breach.

The seven cybersecurity priority areas for the School Leadership team are:

1. Controlling access to key systems and data
2. School network/WiFi security, other systems
3. Software and application security updates
4. Protecting computing devices
5. Data backups and recovery
6. Incident response and recovery
7. Cybersecurity awareness and training

The school leadership team needs to review the following relevant documents. Following this review the school should be in a position to start putting place it's own 'School Cybersecurity Policy' based on the '**School Cybersecurity Policy Template**' document provided.

Relevant documents:

1. Assessing School Cybersecurity Readiness
2. Cybersecurity Training For School Leadership (Powerpoint Presentation)
3. Cybersecurity Incident Response and Recovery Guide
4. **School Cybersecurity Policy Template – Key Document**
5. Cybersecurity - Roles and Responsibilities Table

These documents are located in the 'Leadership' section of
https://www.oidetechnologyineducation.ie/technology-infrastructure/data-security/

The authorised individuals/teams who control cybersecurity awareness and training are listed in Table 1 referenced in the school cybersecurity policy.

Cybersecurity awareness and training - for all staff, students and other relevant parties

The second focus area relates to general cybersecurity awareness training, which is relevant to all parties, staff, students and other parties. Cybersecurity needs to be seen as relevant to all everyone in the school. This will include areas including social engineering attacks and threats from malware, phishing and ransomware attacks. It will also include guidance for users as to how they can reduce the risk of cyberattacks, data loss or a data breach.

If the School Cybersecurity team have any questions in relation to Cybersecurity Awareness and Training they can email Oide Technology in Education at ictadvice@oide.ie