Assess Your School Cybersecurity Readiness

Cybersecurity priority areas for schools:
For each of these areas listed here we have provided some self-reflection review questions for schools so that they can assess their own cybersecurity readiness against the threats of cyberattack or a data breach.

- **Overall School Cybersecurity Policy**
- **Controlling access to key systems and data**
- **School network/WiFi security, other systems**
- **Software and application security updates**
- **Protecting computing devices**
- **Data backups and recovery**
- **Incident response and recovery**
- **Cybersecurity awareness and training**

Overall School Cybersecurity Policy:
The goal of this section is to ensure schools have a 'fit-for-purpose' cybersecurity policy in place.
Here are some high level questions in relation to cybersecurity policy:

- Is cybersecurity a high priority for the school leadership team?
- Does the school have a written cybersecurity policy in place?
- Is the coordination of cybersecurity policy the responsibility of a specific individual or team?
- Are there cybersecurity processes in place, and if so in which areas?
- Does the school have a 'no blame' policy in relation to the reporting of cybersecurity incidents?
- Are the cybersecurity policy and associated processes GDPR compliant?
- Is the policy reviewed regularly by the team?

Controlling access to key systems and data:
The goal of this section is to have secure access to school data and systems. Here are some important questions in relation to these areas.

- Does the school cybersecurity policy refer to how it controls access to school data and systems?
- Does the school have a policy and process in place relating to who has access to systems and data, and does this include sensitive data?
- Can only authorised individuals access certain information or perform specific actions regarding school systems?
- Does the school have a process in place regarding managing passwords?

School network/WiFi security, other systems:
The goal of this section is to protect key school services and platforms.
Here are some questions in relation to the security of the school network/WiFi, Learning Management System (LMS), administration system, and financial/payment system.

- Does the school cybersecurity policy and processes refer to how key school systems are protected?

- Does the school have a process in place relating to who controls login access to the school network, WiFi network?
- Does the school have a process in place relating to who controls login access to the school Learning Management System (LMS), administration system and financial/payment system?
- Is the school network divided into sections to limit the spread of a cyberattack from one section to another?
- Has the school a local firewall in place, and is there a process in place to control this firewall?

Software and Application security updates:
Schools use a range of different types of software to support a range of activities. The goal of this section is to ensure software and applications are kept up to date, especially regarding security updates. Here are some questions in relation to software and application security/updates:

- Does the school have a list of software and applications being used by the school?
- Does the school have a policy and process in place to ensure software and applications are kept up to date?
- Who is responsible for ensuring that software updates are successfully carried out?

Protecting Computing Devices:
The goal of this section is to protect devices. Here are some questions relating to this area.

- Does the school cybersecurity policy refer to protecting devices?
- Does the school have a process in place relating to the security of devices including computers and other devices used in the school?
- Does the school use antivirus software to protect devices using Microsoft Windows?
- Do processes refer to how antivirus and device management are used to protect devices?
- Who is responsible for ensuring that these actions are successfully carried out?

Data Backups and Recovery:
The goal of the data security and backups is to protect school data from unauthorised access, damage or loss. This is one of the most critical cybersecurity areas. Here are some key questions relating to the area:

- Does the school cybersecurity policy refer to how data backups are controlled?
- Does the school have a written policy and process in place to regularly backup important school data?
- Who is responsible for ensuring that data backups are carried out?
- How frequently is school data backed up, and is there a process in place to ensure that the backups are up to date and complete?
- Does the school have a documented policy and process in place to regularly test the backup process?
- Are backups stored locally on site or stored in the cloud?
- Has the backup process been tested recently, and was the test successful?
- Does the backup process include backing up both local and cloud based data?

Incident Response and Recovery:
The goal of the incident response and recovery is to ensure that when a cybersecurity incident happens, that the school has a plan in place to respond and recover from the incident. This section refers to how a school plans to respond to a cybersecurity incident. Here are some questions relating to his area:

- Does the school cybersecurity policy refer to how it handles incident response and recovery?
- When a cyber-incident such a ransomware attack occurs, does the school have a written process in place stating how it plans to respond?
- Who is responsible to ensure that the incident response and recovery plan is in place (ie., individual or team)?
- Has the incident response and recovery process been tested recently, and was the test successful?

Cybersecurity Awareness and Training:
Within the school cybersecurity policy the goal of a cybersecurity awareness and training programme is to enable staff and students to better understand both the cybersecurity risks as well as their individual and collective responsibilities, so as to better protect themselves and their school from cyberattacks. Here are some questions in relation to awareness and training:

- Does the school cybersecurity policy include a section on cybersecurity awareness and training?
- Does the school have a suitable cybersecurity awareness and training programme in place?
- Does the school have an up to date Acceptable Use Policy (AUP) in place that is consistent with their school cybersecurity policy?

If the School Cybersecurity team have any related questions on this area they can email Oide Technology in Education at ictadvice@oide.ie