**School Cybersecurity Policy Template**

**School Name:**

**Roll Number XXXXX.**

*Note: This latest version of this document is available on the Oide Technology in Education website at:* [*https://www.oidetechnologyineducation.ie/technology-infrastructure/data-security/*](https://www.oidetechnologyineducation.ie/technology-infrastructure/data-security/)

**Importance of having a school cybersecurity policy**

This document is **a cybersecurity policy** on how we protect our school against a wide range of cyberattacks or a data breach. Having a school cybersecurity policy in place is critical, and is a statement of intent by our school leadership team. This policy is based on the guidance and policy approach recommended by Oide TiE. For more details on this approach, please refer to: <https://www.oidetechnologyineducation.ie/technology-infrastructure/data-security/>.

This policy provides details in a number of key areas on how our school protects itself, our systems and our data from cyberattack.

* Cybersecurity is a top priority for the school leadership team, including our board of management (BOM), in terms of protecting school systems and school data, to reduce the risk of a cyberattack or a data breach.
* This cybersecurity policy is reviewed each year and updated as necessary.
* **The policy clearly describes the school approach to improving cybersecurity in seven key areas, each of which is designed to reduce the impact of cyber-incidents for the school.**
* To encourage staff and students to engage with our cybersecurity policy, and specifically to report incidents rather than conceal them, a ‘no blame’ policy in relation to the reporting of cybersecurity incidents is in place and encouraged.
* Roles and responsibilities of the school cybersecurity team, including those with specific cybersecurity related roles, are clearly outlined.
* Either a named individual or a team is responsible for implementing the cybersecurity policy and related actions in key areas outlined below. This list of named individuals and teams is put in place and updated by the school Principal (or their delegate) and are listed in Table 1 associated with the school cybersecurity policy.
* The policy links to and is consistent with other school policies such as the school Acceptable Use Policy (AUP), the School Data Protection policy and with GDPR principles.

From our school perspective managing cybersecurity initially seemed daunting, however when we reviewed the guidance and policy approach recommended by Oide TiE, this approach seemed realistic and achievable. Also responsibility for the different areas are shared among individual staff and teams in the school, as well as with some other parties, so this encourages school wide engagement.

**The seven cybersecurity priority areas for our school 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**
	* 1. **Policy on controlling access to school key systems and data**

Controlling access to our school systems, resources and physical IT areas is an essential aspect of our cybersecurity policy.

* The school has a policy in place to control access to systems, resources and physical IT areas.
* Access to systems, resources and physical IT areas is based on school roles and responsibilities, where ‘authorised’ staff/other parties need to have access to carry out school related activities, or have access to specific types of data, including sensitive data. This model is generally referred to as ‘role based access control’ (RBAC).
* The school Principal (or their delegate) is responsible for ensuring that a cybersecurity policy in relation to controlling access to systems, resources and physical IT areas is in place.
* All school system accounts with ‘administration level access’ need to be approved by the school Principal, and the number of these ‘admin’ accounts need to be minimised for security reasons, (recommended minimum is two).
* Access to physical areas in the school where critical IT systems and equipment are located, is restricted to authorised staff as listed in Table 1 of the school cybersecurity policy.
* In the process of disposing of IT equipment, including old or faulty computing devices, servers or storage devices, all data stored on this equipment needs to be erased to eliminate a risk of a data breach.
* The authorised individuals/teams who control access to school systems, resources and physical IT areas are listed in Table 1 associated with the school cybersecurity policy.

**School Policy on Authentication/Access**

Authentication is a process to ensure that only users with the correct login/access details are allowed to access digital and online school resources and systems.

* The school has a policy in place to control authentication/login to resources for staff, students/pupils and other relevant parties.
* Relevant school staff are provided with authenticated access to relevant school systems, including school staff WiFi, the school learning management system (LMS), the school administration system, and other relevant systems.
* Students/pupils are provided with authenticated access to relevant school systems, including school student WiFi, the school learning management system (LMS) and other relevant systems.
* In order to protect important and sensitive data ‘Two-Factor Authentication’ (2FA) is mandatory for the school leadership team, the school cybersecurity team, system administrators and school staff for systems including the school learning management system (LMS), the school administration system, and other school systems in order to protect important and sensitive data.
* School email addresses for staff and students use the school domain (for example staff-name-identifier@school-identifier.ie or student-name-identifier@school-identifier.ie .
* The school Authentication/Access policyspecifies how passwords are managed and controlled. In finalising our policy we reviewed Oide TiE’s School ‘Authentication/Access Policy Guide’ and template which includes guidance and recommended good practice for schools. This is available at <https://www.oidetechnologyineducation.ie/technology-infrastructure/data-security/> .
* The school cybersecurity awareness/training programme includes a section on ‘controlling access to school key systems and data’.
* The authorised individuals/teams who control access to school systems, resources and physical IT areas are listed in Table 1 associated with the school cybersecurity policy.
	+ 1. **Policy on Network/WiFi security, LMS, Admin System, other services**

The security of the school network/WiFi system and other critical school systems are essential aspects of our cybersecurity policy. This includes controlling authorised user login access to these important school systems to ensure they are securely configured to reduce the risk of cyber-incident.

* The school security policy for network/WiFi, LMS, Admin and other systems is outlined here.
* Access to school WiFi is set up to have different levels of WiFi access to staff, students/pupils and guests.
* Staff, student/pupil and guest access to school WiFi is via a secure password, which is set up by the school.
* To reduce the risk that external parties could obtain passwords to access WiFi, passwords are changed at the start of every school year, though the school may decide to change them more frequently.
* Our school WiFi is configured securely using secure network protocols, and we have confirmed this with our WiFi technical support provider).
* Any physical areas covered by the school WiFi system that are not required for a significant period of time are switched off, ie., by disabling the wireless access points (WAPs) in these areas.
* ‘Administration’ level access to the school Learning Management System (LMS), the school administration system, the school financial/payment system, and other important school systems are controlled and accessible only to specific named individuals or teams.
* Our school broadband connection is provided by the Department of Education’s ‘Schools Broadband Network’ by supported by Oide TiE’s Schools Broadband Desk and HEAnet. This connection includes education specific content filtering and a firewall, which our school sees as a critical aspect of our cybersecurity infrastructure.
* The authorised individuals/teams who control access to school systems, resources and physical IT areas are listed in Table 1 associated with the school cybersecurity policy.

* + 1. **Policy on Software and Applications security/updates**

Our school uses a number of different types of software and applications to support a wide range of teaching, learning and administration activities. To minimise the risk of cyberattack via the software and applications we use, it is important that where possible, we are using the latest versions of software, which include the latest cybersecurity updates.

* The school policy to ensure software and applications are kept up to date, is outlined here.
* The school maintains a list of online platforms, software and applications being used in the school.
* Software operating systems, applications and services are regularly updated, where possible, to improve their cybersecurity resilience against cyberattack.
* Our school policy is to enable software ‘automatic updates’ where appropriate to do so, for example for Microsoft products ‘automatic updates’ are always enabled.
* The authorised individuals/teams who ensure software and applications are kept up to date are listed in Table 1 associated with the school cybersecurity policy.

* + 1. **Policy on Protecting Devices**

Protecting school devices is an essential aspect of our school cybersecurity policy.

* The school policy in relation to protecting schools devices, including data stored on these devices is outlined here.
* The school ensures that where possible, Operating System (OS) software used by the school is kept up to date on computing devices, and on any servers being used within the school.
* The school ensures that any Anti-Virus (AV) software being used on school Microsoft Windows devices is kept up to date, and set to update automatically.
* The school carried out a risk assessment regarding portable school devices including laptops, smartphones, USB keys and other portable storage devices. The school recognises that such portable devices, which may store important school data, pose an increased data breach risk, if they are lost, stolen or compromised.
* Given the serious negative impact of such an incident happening, the school has a policy that no important school data is allowed to be stored on portable devices such as laptops, USB sticks or other storage devices.
* In exceptional circumstances where portable devices are approved to store important school data, these devices have encryption turned on, to lower the risk of a data breach.
* As the school is using Windows 11 Professional Operating Systems on school Desktop PCs and Laptops and are also using Microsoft 365 (with A3 licences), we have decided not to have an additional third party anti-virus (AV) software of these devices. This is not just a cost saving exercise. Our view is that no anti-virus software can guarantee protection against viruses so we feel that the additional AV cost does not justify any potential benefits.
* The school also uses Chromebooks and Apple devices. As these are generally considered a ‘lower risk’ of being infected by ‘viruses’, we don’t use AV protection software on these devices. However we understand that these devices are still at risk from other cyberattacks including phishing, so this aspect is included in the school cybersecurity awareness and training plan.
* To protect Chromebook devices only Chromebook approved ‘apps’ from the ‘Google App Store’ are allowed to be downloaded to these devices.
* To protect Apple devices only Apple approved ‘apps’ from the ‘Apple App Store’ are allowed to be downloaded to these devices.
* The authorised individuals/teams who are responsible for the policy on protecting devices are listed in Table 1 associated with the school cybersecurity policy.
	+ 1. **Policy on Data Backup and Recovery**

This is a critical cybersecurity area in protecting our school data from unauthorised access, data loss or data breach. The following are some important points in relation to our data backup and recovery policy and actions.

* To reduce the risk of permanent loss of important school data due to malware, equipment failure, or other causes, the single most important step that our school has in place is to carry out regular ‘standalone’ backups of important school data.
	+ A standalone backup is one that is stored in a separate, disconnected and/or ‘off-site’ location, so that if the original data is lost or inaccessible, the school still has a copy of the data.
	+ The ‘standalone’ location could be a separate drive or could be on a ‘cloud based’ service.
* The school has a policy in place to ensure a robust and regular data backup and recovery process.
* The school has identified specific important data/files/folders and systems that require daily backup.
* The school uses a high quality ‘cloud backup’ as the main school data backup service.
* The school policy requires that automated data backups are carried out to a cloud backup service, ‘at least’ on a daily basis.
* To reduce the risk of a ransomware attack data backups are physically separate and disconnected from the main data store.
* Data backups are required to be carried out and tested before making significant changes to critical systems involving important school data. These critical systems include school databases, LMS, Administration system, payment systems etc.
* Other additional data backups may be carried out automatically or manually.
* While a data backup process is critical, being able to restoring data from backups (the recovery process) is equally important.
* Testing of the data backup and recovery process is carried out regularly, to ensure it works successfully.
* The authorised individuals/teams who control data backup and recovery are listed in Table 1 associated with the school cybersecurity policy.

* + 1. **Policy on Incident Response and Recovery**

The school has a written cybersecurity incident response and recovery policy in place to ensure that when a cybersecurity incident or data breach happens, the school already has a plan in place outlining how it will respond. Having a plan already in place minimises the impact to the school, so as to recover school systems and data as quickly as possible.

* This guiding plan outlines our school response to improve the schools preparation in key areas.
* The school leadership team is responsible for having the incident response and recovery plan in place.
* The roles and responsibilities of the incident response and recovery team are clearly identified, understood and accepted by the team.
* The authorised individuals/teams who are responsible for and coordinate the incident response and recovery plan are listed in Table 1 associated with the school cybersecurity policy.
* **The most urgent priority is to ensure that the school policy on data back and recovery is active, and up to date. This is to ensure that data backup are protected from being deleted, damaged or corrupted by a cyberattack. Refer to the data backup and recovery policy for relevant details.**
* Part of our incident response and recovery planning process is to have already carried out an **‘cyber-incident simulation exercise’** which is activated and pre-tested during the first term of each school year. The purpose of this ‘incident simulation exercise’ is to improve how the school can prepare in advance for a possible cybersecurity attack or data breach, and to minimise any issues or ‘panic’ that might otherwise occur, during an actual cyber-incident.
* In finalising our policy in this area we reviewed Oide TiE’s Incident Response and Recovery guidance and template, which recommends good practice in this area for schools. Oide TiE’s ‘Incident Response and Recovery Guide’ is available at: *https://www.oidetechnologyineducation.ie/technology-infrastructure/data-security/*
* If an actual cybersecurity incident is suspected, the team leader of the cybersecurity incident response team (or their delegate) will call an urgent meeting (either in person or remotely) to assess the situation and to decide on next steps.
* If an actual cyber incident or data breach does seem to have happened, then the cybersecurity incident response and recovery plan is activated. This gives the go-ahead for a series of already-planned and approved specific actions to take place.
* These actions are designed to protect the school systems and data, to minimise the impact of a suspected cyber-incident on the school and school community.
* Other priority measures include turning off/disabling the school network, school computers, WiFi and Broadband from the ‘outside world’, so that all school digital and online systems are no longer available or accessible. This disables user access to all online school systems.
* Testing of the incident response and recovery plan is carried out at least annually, to ensure it is up to date.
	+ 1. **Policy on Cybersecurity Awareness and Training**

The school leadership team understand the importance of having a Cybersecurity Awareness and Training programme in place in the school. As a result it has prioritised the need to have a cybersecurity awareness and training programme in place 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 school has a written cybersecurity awareness and training plan in place.
* The training programme is consistent with other school policies such as the 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 school leadership as well as training regarding specific responsibilities. 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 our 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 schools 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 authorised individuals/teams who control cybersecurity awareness and training are listed in Table 1 associated with the school cybersecurity policy.

**Cybersecurity awareness and training - All 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 related questions on this area they can email

Oide Technology in Education at ictadvice@oide.ie