# GCSN – Sample Cyber Safety Action Plan

**How to Use This Plan:**

This plan is intended to be used as a guiding template for schools and kura to form their own cyber safety action plans, in accordance with their priorities as a school, their vision and values, their unique context and special character, and their history of IT safety breaches and security concerns.

The sample information can be kept, removed, and edited to reflect the context of the school or kura and ensure that the plan is unique to the school/kura and used to inform ongoing mitigations and actions performed across the school. Schools and kura may choose to add or remove columns as they see fit, and adjust the levels of risk and impact.

The grey text provides contextual information for what information should be included in each column. We recommend this is kept in order to inform future plans, assist in making edits as necessary, and ensure that the plan can be understood by others.

|  |  |  |
| --- | --- | --- |
| **Date of Update** | **Notes** | **Next Scheduled Update** |
| Date or date range of edits and updates made to this plan.  | What was done in the latest update. Consider the evolving nature of threats, consequences, likelihood of events etc. Digital Technologies can evolve with time so plan to review this plan and make adjustments regularly. | Date of when the document should be reviewed and updated. Be sure to set reminders. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

| **Threat** | **Consequence** | **Likelihood of occurring** | **Impact** | **Mitigating factors** | **Actions** |
| --- | --- | --- | --- | --- | --- |
| *Briefly describe the threat.* | *Outline the consequences of the threat should it occur.* *Consider: Operational disruption, data loss/privacy breach, financial loss, reputational harm, and harm directly to students.* | *1-5 scale, where 1 = low risk, 3 = medium risk, and 5 = high risk of happening.*  | *Consider the potential impact and provide a scale range of 1-5.*  | *Briefly describe what measures are currently in place to mitigate the threat and reduce impact. Specify which are already in place and which are not yet in place. This will inform the actions in the next column.* | *Outline steps to upgrade mitigations, continue upskilling in this area and manage threats or crises as they occur.* *Review these on a termly basis to ensure they are up to date. Note which mitigations are in place and which are yet to be explored.*  |
| Human error in sharing confidential or sensitive information. | **Data/Privacy Breach**Confidential or sensitive information on staff, students, or private school information may be shared without permission, or may be accessed by a malicious third party. **Reputational Harm**Sharing such data or information may create misunderstandings, embarrassment, conflict, or be a direct breach of privacy. |  |  | *Delete, add to, and expand on the following.***Mitigations in place:****Mitigations required:*** Staff PLD addresses cybersafety and digital citizenship.
* Staff onboarding addresses responsible use.
* Responsible use agreements in place.
* Ākonga cybersafety education.
* Access control on sensitive data.
* Passwords regularly updated.
 | *Delete, add to, and expand on the following.*Cybersafety and responsible use agreements are renewed each year and cocreated with staff so they are aware of their responsibilities to keep data safe.Breaches in confidentiality are dealt with quickly and discretely where possible. Where breaches occur, those responsible are educated on how to avoid such problems in the future.Staff are continually reminded of e-mail etiquette and safe use. Cybersecurity education is integrated into the local curriculum and continually renewed to include modern threats. IT staff are responsible for introducing access controls, including removing access privileges for staff leaving.  |
| Phishing scam. | **Data/Privacy Breach**Untrustworthy links may be clicked, or sensitive information such as passwords, bank account numbers, names or other data may be shared with malicious third parties.  |  |  | *Delete, add to, and expand on the following.***Mitigations in place:****Mitigations required:*** Staff PLD addresses cybersafety and digital citizenship.
* E-mail software has spam filters and threat detection.
* Staff report suspicious e-mails to IT.
* Potential scams and attacks are regularly communicated to staff.
* Responsible use agreements in place.
* Ākonga cybersafety education.
* Passwords regularly updated.
 | *Delete, add to, and expand on the following.*Responsible use agreements and PLD addresses how staff report suspicious e-mails to senior leaders and IT staff.Senior leaders and IT staff report to students and staff about potential scams and attacks regularly.Cybersecurity education addresses threat detection and ākonga are taught to report suspicious e-mails and contacts that could be phishing. Where breaches are made, threats are contained and appropriate action is taken, including informing the people responsible on how to avoid such threats in the future.  |
| Denial-of-service (DoS) attack. | **Operational Disruption:**School servers or network shut down due to flooded requests. **Data/Privacy Breach:**This may allow a malicious third party to access confidential data without being traced. Ākonga may initiate such attacks to disrupt school systems. |  |  | *Delete, add to, and expand on the following.***Mitigations in place:****Mitigations required:*** Digital citizenship integrated into ākonga education.
* Passwords regularly updated.
* System software and operating systems are regularly updated.
* School systems have threat detection software.
* Staff and student devices are routinely equipped with threat detection software.
 | *Delete, add to, and expand on the following.*Digital Technologies curriculum covers cyber threats including DoS attacks and ākonga are encouraged to be digital citizens.Staff are informed of attacks and are encouraged to quickly report potential breaches so they may be dealt with. Our communications policies quickly inform staff, students, and whānau of DoS attacks and how to protect their data.Our IT staff and service providers are quickly mobilised when a DoS attack occurs to contain the issue and recover data.We regularly update our school systems and staff and student devices with threat detection software. We ensure devices and operating systems are regularly updated. |
| Malware, ransomware and viruses. | **Operational Disruption and Data/Privacy Breach:**Malicious software could infect school systems, staff and student devices, causing harm to existing data and processes.  |  |  | *Delete, add to, and expand on the following.***Mitigations in place:****Mitigations required:*** Digital citizenship integrated into ākonga education.
* Passwords regularly updated.
* System software and operating systems are regularly updated.
* School systems have threat detection software.
* Staff and student devices are routinely equipped with threat detection software.
 | *Delete, add to, and expand on the following.*Digital Technologies curriculum covers cyber threats including malware, ransomware and viruses, and ākonga are encouraged to be digital citizens.Staff are informed of attacks and are encouraged to quickly report potential breaches so they may be dealt with. Our communications policies quickly inform staff, students, and whānau of breaches and how to protect their data.Our IT staff and service providers are quickly mobilised when a breach occurs to contain the issue and recover data.We regularly update our school systems and staff and student devices with threat detection software. Viruses scans are routinely run.We ensure devices and operating systems are regularly updated.We provide resources on an ongoing basis for whānau about how to keep themselves safe online. |
| Cyberbullying / cyberstalking. | **Harm to Students:**Ākonga target one another with bullying online or using digital technologies. Affected ākonga may face extreme wellbeing issues in the future.Cyberstalking may place ākonga at risk outside of school. |  |  | *Delete, add to, and expand on the following.***Mitigations in place:****Mitigations required:*** Digital citizenship integrated into ākonga education.
* Certain websites are inaccessible through network blocks, including sites where bullying is perpetuated.
* Online safety information is available to ākonga and whānau to encourage safe online use.
* Responsible use agreements in place.
 | *Delete, add to, and expand on the following.*Digital Technologies curriculum covers digital citizenship to ensure that ākonga understand acceptable and unacceptable online behaviours and proactively stop bullying behaviours.Responsible use agreements are co-designed with ākonga to cover a range of unacceptable online behaviours and ensure that ākonga are responsible for the way they use the internet. Bullying incidents are dealt with quickly and restorative practices ensure that ākonga are responsible for their behaviour online. We provide resources on an ongoing basis for whānau about how to keep ākonga safe online. |
| Sharing of inappropriate material. | **Harm to Students:**Ākonga are exposed to adult, violent, or other inappropriate material shared via technology without staff awareness.  |  |  | *Delete, add to, and expand on the following.***Mitigations in place:****Mitigations required:*** Digital citizenship integrated into ākonga education.
* Certain websites are inaccessible through network blocks.
* Online safety information is available to ākonga and whānau to encourage safe online use.
* Responsible use agreements in place.
 | *Delete, add to, and expand on the following.*Digital Technologies curriculum covers digital citizenship to ensure that ākonga understand acceptable and unacceptable online behaviours and do not access or share inappropriate material.Responsible use agreements are co-designed with ākonga to cover a range of unacceptable online behaviours and ensure that ākonga are responsible for the way they use the internet. Incidents of sharing inappropriate material are dealt with quickly and restorative practices ensure that ākonga are responsible for their behaviour online.We provide resources on an ongoing basis for whānau about how to keep ākonga safe online. |
| Failure of school service provider. | **Operational Disruption:**Disruption to the functioning of school systems including network and security.**Data/Privacy Breach:**Disruption to systems could result in data becoming vulnerable while systems are recovered or new systems are put in place.**Financial loss:**Potential financial loss to change providers.  |  |  | *Delete, add to, and expand on the following.***Mitigations in place:****Mitigations required:*** School leadership has contracts with service providers.
* Service providers provide routine maintenance/checkups and adhere to a schedule.
* School has access to emergency contacts in the event of a system failure.
 | *Delete, add to, and expand on the following.*Senior Management have contracts drawn up with service providers, minimising the potential impact of a loss of service.Emergency contacts are provided so schools have quick contact in the event of a system failure. Where there is a transition between providers, this is planned to ensure there is no time where systems are absent or unprotected. |
| Online grooming and predation. | **Harm to Students:**Ākonga are subject to unlawful acts and solicitation from adults. |  |  | *Delete, add to, and expand on the following.***Mitigations in place:****Mitigations required:*** Digital citizenship integrated into ākonga education.
* Certain websites are inaccessible through network blocks.
* Online safety information is available to ākonga and whānau to encourage safe online use.
* Responsible use agreements in place.
 | *Delete, add to, and expand on the following.*Digital Technologies curriculum covers digital citizenship to ensure that ākonga understand acceptable and unacceptable online behaviours and know how to keep themselves and their information safe.Responsible use agreements are co-designed with ākonga to cover a range of unacceptable online behaviours and ensure that ākonga are responsible for the way they use the internet. Ākonga are encouraged to share incidents with inappropriate online behaviour and such incidents are dealt with quickly and with dignity.We provide resources on an ongoing basis for whānau about how to keep ākonga safe online. |
| Zoom bombing. | **Operational Disruption:**Online learning is disrupted by external people.**Harm to Students:**Worst case scenario these incidents can result in ākonga being exposed to inappropriate material when learning through video-conferencing. |  |  | *Delete, add to, and expand on the following.***Mitigations in place:****Mitigations required:*** Video-conferencing software uses appropriate security including passcodes and waiting rooms.
* Responsible use agreements in place.
* Staff PLD addresses cybersafety and digital citizenship.
* Online learning policies are designed to quickly shut down zoom bombing.
 | *Delete, add to, and expand on the following.*Online learning always uses passcodes and waiting rooms, and kaiako admit ākonga prior to starting the lesson ensuring no one uninvited can join.In the event a video-conference call is zoom bombed, kaiako are aware of how to quickly shut it down and keep ākonga safe. Incidents are reported to IT staff and senior leadership. |
| Loss or corruption of data. | **Operational Disruption and Financial Loss:**Important information, records, materials, and assessment is lost due to an error, system crash, or other reason. Corrupted data may be unrecoverable. |  |  | *Delete, add to, and expand on the following.***Mitigations in place:****Mitigations required:*** Backup protocols are in place to backup important information to the cloud.
* Staff PLD addresses cybersafety and data protection.
 | *Delete, add to, and expand on the following.*Backup protocols cover how important data is protected online. This data is regularly checked, cleaned, and organised. PLD covers how staff can keep information safe, backed up, and protected in the event of random loss or corruption.  |

# Risk Matrix

The following risk matrix considers the likelihood of occurring and impact, each scored out of five. These can be plotted on the risk matrix below to identify which threats require ongoing monitoring of mitigating factors. You may use this to colour-code threats for quick identification.

|  |  |  |
| --- | --- | --- |
|  |  | Impact |
|  |  | Negligible | Minor | Moderate | Significant | Severe |
| Likelihood | Very likely | Low – Medium | Medium | Medium – High | High | High |
| Likely | Low | Low – Medium | Medium | Medium – High | High |
| Possible | Low | Low – Medium | Medium | Medium – High | Medium – High |
| Unlikely | Low | Low – Medium | Low – Medium | Medium | Medium – High |
| Very unlikely | Low | Low | Low – Medium | Medium | Medium |