HORIZON
CYBER SECURITY

Cyber security policy and procedures

Information Technology

1. Introduction

Purpose and Scope

The purpose of this document is to provide a single, formal reference for the management of all information technology resources for Horizon Christian School

This generalised policy is to be read in conjunction with school policies, the Compliance Programme and the Risk Management Programme, as well as the appendices to this policy. All current and future staff, including contractors and/or temporary/part-time employees, are governed by the contents of this policy.

Annual Review

This Policy and its underlying processes and procedures must undergo a formal review, at least annually, by ICT Management.

The review must consider the context of the School's strategic plans for the coming year and will include the following topics at a minimum:

- security of information
- the currency, quality and relevance of the School's IT systems
- disaster recovery and School continuity arrangements
- the number of users on the system
- system response and down times
- any complaints received that somehow relate to the School's IT systems

Any changes arising from the review and any other changes occurring throughout the year for operational reasons must be rolled out through the School as per the process outlined in the School's compliance programme.

2. General Security Framework

Information security training

All representatives to the School are required to undertake and maintain working knowledge of basic information security protocols. All new School representatives will be provided with a training segment on information security as part of induction training.

This training covers all the general subjects of this policy including:

- Hacking
- Virus Awareness
- Phishing
- Social Engineering
- Passwords
- Multifactor Authentication
- Use of Wi-Fi
- Use of USB Keys
- Physical security
- Reporting of security events

Information security responsibility

All staff and representatives of the School are also responsible for contributing to the School's security by being aware of the relevant security policy and procedures to their position. Where a potential security issue is identified, ICT Management is to be informed of the breach so appropriate action can be taken.

Breach of policy

Maintenance of security in the School is important and conversely not taking security seriously could have significant detrimental impact on the School. Any breach of the IT policy will be treated seriously and will result in severe corrective action being taken, up to and including termination of ICT arrangements with the party in breach.

Fraud

The School reserves the right to suspend our staff and representatives suspected of fraudulent activities pending completion of a full investigation.

Any time fraudulent activity is suspected to be occurring, the details will be fully investigated and if warranted, handed over to the Police. If a staff member is found to be implicated in fraudulent or illegal activity, it is the School's responsibility to cooperate with the authorities fully.

Disposal of IT equipment

Any IT equipment that is determined to be no longer suitable for use must be disposed of in a secure way by qualified IT professionals to ensure all company information is permanently removed.

3. Internet & network access

Personal responsibility

The School provides connection to the Internet to enhance School communications and to provide access to a wide variety of services that may be beneficial to the School.

The Internet is however a distrusted network and staff are expected to act in a responsible, security conscious manner in relation to all use of the Internet. If there is any doubt about the security of any action then "DON'T DO IT."

Some of the policy in this section may overlap with other policies e.g. Network, however because the Internet is such an important tool BUT also provides the greatest potential to compromise security, it is considered important to specifically state policies related to Internet access in addition to other policies and with a particular focus on individual responsibility.

Provision of internet services

Internet access is provided by the School to facilitate with School work/teaching. The use of the Internet for email, file transfer, information browsing, remote host login, etc. is intended primarily for School purposes.

Access from School systems

Internet services have been designed with security as a key factor. Staff must use the standard process when accessing the Internet from any device and not bypass any security measure.

Access to the Internet via non-standard methods such as dial-up to an alternate Internet Service Provider (ISP) will only be permitted based on specific School needs and after management approval. In such cases additional security measures need to be applied.

Staff must ensure that they use access to the Internet is in a responsible manner. Care must be taken in relation to all Internet activity including any access to school web pages, sites and systems accessed, data downloaded, messages and other transmissions over the Internet. Nothing which could impact the security of the School's network or reputation should be attempted.

Portable IT equipment

Those staff issued with company owned laptop computers, tablets and USB devices must ensure the physical security of the device such as ensuring it does not get left in taxi's or on public transport and that it is always protected from any physical damage or theft.

Users are personally responsible for the security of information stored on portable IT devices. The user must immediately report the potential loss of theft of a portable IT device and data to their manager.

VPNs

Approved staff may remotely connect to the school network and resources with appropriate approvals and School needs. VPN technology provides an encrypted tunnel through a public network so information transmitted to and from systems are not easily readable by unauthorised parties.
Staff using VPN connections are responsible for their remote Internet Service Provider (ISP), the security of the device they are using to run the VPN software and coordinating the installation of school approved VPN software.

Internet of Things (IoT) Devices

IoT devices covers anything not PC's and Servers, this could be Smart TV's, CCTV systems etc. Items such as these and other network connected devices must be secured on the network or segregated from other production environments. Firmware updates must also occur regularly on these devices to ensure any security patches are applied.

Access to external systems

When utilising our School systems to access third party computer systems, staff must comply with all applicable guidelines of the accessed system. Attempts to access any system without valid authority are prohibited.

Sensitive information

Sensitive information' is defined in the Privacy Act to mean information or an opinion about an individual's:

racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices or criminal record.

Sensitive information also includes health information and genetic information about an individual that is not otherwise health information, financial information and other personally identifying information such as passport or drivers licence numbers.

Take precautions when sending sensitive, confidential or proprietary information over the Internet unless it is encrypted. If you are uncertain whether material is sensitive, confidential or proprietary, consult your ICT manager. If you need to send sensitive, confidential or proprietary information electronically and encryption is not available, alternate ways of transmitting/sending this information should be used.
Discuss this with your ICT manager/support for options.

Email usage

The School utilises antispam software to filter out the majority of email threats, but it is still extremely important to verify incoming emails are legitimate. All care should be taken to specifically ensure any email that requests financial payment, confirmation of password, prompts for a login to Microsoft 365 etc are verified as genuine by calling the sender or forwarding to IT Support before any other action is taken.

Illegal or offensive materials

Internet users shall comply with applicable statutes, regulations and School policies and procedures including those that require an employment environment free from discrimination and harassment. Consistent with this, we expect personnel to exercise common sense and judgment to avoid any communication which is disrespectful or offensive to others or which is illegal.

While our School does not intend to stifle free expression or censor employee communication, the School, as the access-provider to the Internet, reserves the right to specify how School network resources will be used and administered to comply with these guidelines and to maintain a work climate consistent with our School values.

Personal internet use

Internet access is provided to facilitate the School's learning process within the classroom and administration. Personal use is acceptable given general benefit to the school by promoting enhanced staff morale and working conditions, but should not interfere or conflict with School use.

Personal Internet use should be considered similar to making personal telephone calls while on the job. It is unacceptable spending excessive time on the telephone for personal reasons; the same applies to accessing sites on the Internet for personal information.

User passwords - guidance

User Passwords should:

- Be a reasonable strength and as a minimum:
    - Be at least 8 characters long
    - Contain a mix of alpha and non-alpha characters
- Initial password allocation must be randomly and uniquely generated
- Not be recycled.
- Be stored encrypted, using one-way encryption if possible and exceptions documented.
- Not be displayed or printed.
- Not be divulged by the user.
- After a user password is set by an administrator (e.g. password reset, or new user's initial password) the user must change their password at first successful login.

The use of passwords has become quite pervasive with the advent of the Internet, with numerous services being offered such as personal email, lists, social media, instant messaging, to name a few. It is common for users to have "favourite" passwords which they use over multiple systems and environments. It is also common for "hackers" to exploit the reuse of

passwords, so if a password is discovered this potentially compromises all systems on which this password is used.

The security of a password is only as strong as the weakest environment in which it is used. As there is no guarantee of the security of non-Company environments, any password used within the Company must not be used on any system outside Company control.

Use of a secure password management tool is considered best practice for storing credentials, these can be integrated into internet browsers and mobile apps and secured with their own password. Trusted providers of these tools include Bitwarden, LastPass and Roboform. Storage of passwords in Excel documents is to be avoided at all costs.

Multifactor Authentication

With new technological advances it is easy for individuals to inadvertently fall victim to highly sophisticated phishing attacks or for credentials such as username and passwords to be compromised. This could give a third-party unauthorised access to our network and information system (Network).

Multifactor authentication where available should be used and a preference be for using MFA software such as Microsoft Authenticator and Google Authenticator.

4. School Continuity Planning

A School Continuity Plan is a document that defines the policies and procedures for dealing with various types of disasters that can affect the schools data, especially the organisation's Technology infrastructure. A disaster is any event that has a significant impact on a School's ability to conduct operations. It is recommended that all staff are aware of the School's Continuity Plan and their roles within it.

5. Appendix A – Annual IT Review

Passwords & Security			
Test	**Description**	**Response**	**Corrective Actions (Where appropriate)**
Password Complexity	Complex passwords are used. At least 8 Characters long containing Uppercase, Lowercase, a number and a symbol. Passwords to key systems are not re-used on less secure sites. Smartphones should be password protected	☐ Yes ☐ No	Action: Due Date: Assigned to:
Password Management	Passwords are not recorded in an unencrypted format digitally, or in paper in a similar location to digital devices (e.g. excel spreadsheets, post-it notes on computers). Password management tool in use.	☐ Yes ☐ No	Action: Due Date: Assigned to:
Unique Users	Unique log-ins for all members of staff that need to access key systems and programs, so that individual work can be tracked. Logs of access to sensitive data are recorded and stored in a secure environment.	☐ Yes ☐ No	Action: Due Date: Assigned to:
User Clean-up	Have user permissions been reviewed, and unnecessary accesses removed?	☐ Yes ☐ No	Action: Due Date: Assigned to:

Security Software	Utilisation of anti-virus software in addition to anti-malware exploit scanning completed at least once per month	☐ Yes ☐ No	Action: Due Date: Assigned to:
Security Updates	Is all security software set to automatically update?	☐ Yes ☐ No	Action: Due Date: Assigned to:
Software patching	Is all software patching up to date for computer operating systems and third-party software? Is this conducted automatically?	☐ Yes ☐ No	Action: Due Date: Assigned to:
Internet of Things Devices	Is the firmware on all IoT devices up to date? Are the devices secure on the network?	☐ Yes ☐ No	Action: Due Date: Assigned to:
Multifactor Authentication used where possible	Is MFA enabled wherever possible for online systems containing client or School sensitive information?	☐ Yes ☐ No	Action: Due Date: Assigned to:
Backups	Is ALL data backed up daily?	☐ Yes ☐ No	Action: Due Date: Assigned to:

Networking & Hardware Security

Test	**Description**	**Response**	**Corrective Actions (Where appropriate)**
Secure Networks Only	School rules prevent access of public Wi-Fi (e.g. airports and hotels). Use only private connections such as mobile tethering.	☐ Yes ☐ No	Action: Due Date: Assigned to:
Hardware passwords	Ensure all devices such as modems and wireless networks do not still use the default password	☐ Yes ☐ No	Action: Due Date: Assigned to:

Computer lockout	Ensure all computers are locked when not in use, and are set to automatically lock after a period of non-use.	☐ Yes ☐ No	Action: Due Date: Assigned to:
Unknown USB devices and cables	USB devices and cabling from unknown sources are not plugged into computers	☐ Yes ☐ No	Action: Due Date: Assigned to:
Firewall	Is a secure firewall in place on the network?	☐ Yes ☐ No	Action: Due Date: Assigned to:

Resourcing			
Test	**Description**	**Response**	**Corrective Actions (Where appropriate)**
IT-Related Complaints	Has the School received any complaints in relation to its digital systems?	☐ Yes ☐ No	Action: Due Date: Assigned to:
Security Awareness Training	Have all staff undertaken security awareness training in the past 12 months?	☐ Yes ☐ No	Action: Due Date: Assigned to:
School Continuity Plan	Is the School's plan in the event of a disaster effectively a combination of the following: - An identified group of people with responsibilities assigned for finance, communication and decision making with backup representatives - Replacing/repairing hardware - Operating remotely - Restoring data from the backup	☐ Yes ☐ No	Action: Due Date: Assigned to:

Outdated Systems	Does the School utilise any systems which are out-of-date and at risk of no longer being fit-for-purpose?	☐ Yes ☐ No	Action: Due Date: Assigned to:
Scalability	Holistically, does the School have the IT systems in place to meet its needs for the next 12 months?	☐ Yes ☐ No	Action: Due Date: Assigned to:
Insurance	Does the school have appropriate technology insurance in place? i.e. Cyber Liability Insurance	☐ Yes ☐ No	Action: Due Date: Assigned to:
IT Review Result	Overall, based on this report, the School' IT Resourcing is rated:	☐ Unsatisfactory ☐ Needs Improvement ☐ Satisfactory	Action: Due Date: Assigned to:
Further Actions	Are there additional matters that should be considered within the School's IT review?	☐ Yes ☐ No	*Narrate accordingly below*

Comments:

The School....