Policy

Use of Information and Communications Technology (ICT) Resources

HEREWORTH
DESIGNED FOR BOYS

Background
This policy is necessary in order to:

- Provide all Hereworth members (Board, staff, boys and volunteers) with clear parameters for the acceptable use of Hereworth technology (e.g. internet, email, mobile devices) equipment and/or information and social media sites, whether for business or personal use.
- Ensure the publication of any images or commentary on social media sites and platforms (i.e. any internet based tools used for publishing, sharing and discussing information) by members of Hereworth reflects the values and views of the organisation and does not negatively impact on its reputation and public trust and confidence.

Purpose
This Policy is designed to achieve the following:

Technology, resources and information repositories are provided and maintained to enable members to carry out legitimate Hereworth business associated with their role. Access to these resources is available to support effective work practices, communication, research and information-seeking/ sharing activities directly associated with meeting Hereworth business / organisational needs.

Guidelines

Responsibilities and Authorities
The policy applies to all members (paid and volunteer) and anyone else (e.g. contractors) authorised to have access to Hereworth technology and/or resources, or when using social media or other public sites in their work with Hereworth.
Managers are responsible for ensuring that any newly engaged team members and/or contractors (or other third party users) are made aware of their rights and responsibilities under this policy and related procedures. In regard to the use of Hereworth technology and resources, members should have no expectation of privacy - including the privacy of private communications made on or through its systems.
All users of Hereworth telephone, cell-phone, computer systems and/or equipment are required to:
• Familiarise themselves with this policy and comply with its terms.
• Take any other necessary steps to ensure that Hereworth technology and/or resources or social media sites are not used in ways that would expose the organisation to risk, harm its reputation/image and/or jeopardise its operation or the availability of its resources.

Non-compliance or failure to adhere to this policy - or any inappropriate use of social media or Hereworth internet, email or telephone systems - will be viewed very seriously and disciplinary action may result, up to and including dismissal or the termination of membership.

Acceptable Use
Email is a written means of communication. Members should not transmit anything in an email message that they would not write in a letter or memorandum.

Access to the internet and other information repositories, cell-phones/landlines are provided for work and research purposes to help meet Hereworth's objectives; therefore their primary use is for Hereworth business, generally during the member's prescribed hours of work.

Acceptable use of technology (including cell-phones and mobile devices provided by Hereworth), photocopiers, cameras, data-shows and other equipment, resources and information/repositories includes the following activities which must have a direct association to Hereworth's business:

- Communication and collaboration with colleagues, clients, stakeholders and health sector partners.
- Administrative communications/activities.
- Work and research.

All activities must be conducted in a manner consistent with Hereworth's values and normal standards of business, behaviour and communication.

Access to the Internet
To help maintain security and avoid the spread of viruses, users must access the Internet only via Hereworth Internet gateways and firewall. Access via modem from a workstation is strictly prohibited except when dialling into the Hereworth network using approved dial-up procedures (e.g. laptop being used remotely) or dialling up by an approved organisation for a specific business purpose.
All special purpose dial-ins will require set up via a Hereworth Information Communications and Technology (ICT) staff member or an authorised Hereworth vendor (i.e. TeamViewer).

Personal Use of Hereworth Systems
Users may make limited personal use of Hereworth systems, technology and equipment under the terms outlined in this policy. Such use is a privilege and may be revoked if abuse is found to have taken place; in serious cases disciplinary action may result.
Personal use is to be:
- Reasonable in scope and duration.
- Undertaken in the member's own time (e.g. during meal/refreshment breaks or before or after business or rostered work times – unless of a very short duration (e.g. a short telephone call).
- Kept to a minimum and not interfere with the performance of required duties.
- Consistent with any management permissions and terms.
- Not incur any direct cost for Hereworth.
- Not impede or interfere with use of the system/resource for other work purposes and/or by other individuals.
- Consistent with Hereworth's values and the behaviour and communication expected of its members.

This limited approval does *not* apply to the use of Hereworth information for private purposes.

Unacceptable use of technology, resources and information includes but is not limited to:
- Use for personal profit activities.
- Any use which interferes with the integrity of Hereworth computer systems, both within the intranet, the organisation or on the wider internet.
- Accessing illicit and /or adult sites or any site not appropriate for work-related activity; and downloading, storing and/or forwarding any such materials.
- Objectionable use – including the storage or forwarding of email or text/photographic or other imaging that is illicit, offensive, indecent, racist, sexist, abusive, derogatory, defamatory or of a bullying or harassing nature. Political or nuisance emails or texts also fall into this category.
- Conducting any illicit/illegal activity.
- Any use which invades the privacy of others.
- Sending or forwarding inappropriate/offensive or nuisance texts, comments, images or materials.
- Advertising of any kind unless specifically related to Hereworth announcements, new products or services, approved by the relevant manager; or that within mailing lists and new groups or public folders which allow advertising.
- The downloading, installation or use of non-approved software or games from the internet or other sources.
- Disclosing patient / client or member details (e.g. scenes, photos of accident) without appropriate

permission.
- Making comments or transmitting information that may discredit Hereworth or damage its reputation.

If a member becomes aware of an inadvertent breach of this policy on their own part, they should advise their manager as soon as practicable.
Members are required to address any perceived misuse of technology by others – either with the individual if the use is seen to be inadvertent or trivial - or with the relevant manager (for guidance and any necessary investigation/follow-up) if concerns are more serious in nature. In such situations the Headmaster must refer to the Act to ensure we follow the Act's process.

Usage Monitoring
Hereworth reserves the right to monitor member usage of its resources and systems and to take appropriate action to address any excessive or unacceptable use as it sees appropriate, including investigative and disciplinary action.
Browsing reports will be produced and reviewed on a regular basis; they will identify specific internet activity to individual users.
Hereworth will retain back-up copies of all documents, including email correspondence produced on its computer system. Members should therefore be aware that deleting an email message or browser history does not guarantee erasure from the system.
If it becomes necessary to examine member usage as part of an investigation (e.g. as part of a required disciplinary or criminal investigation) established forensic protocols and tools will be used to recover information.

Security
Members must abide by security restrictions on all information and systems to which they have access. Attempting to evade, disable or "crack" passwords, revealing a password or other security provisions threatens the work of others and is therefore unacceptable.
If access to information is required, explicit authorisation must be obtained from the appropriate department or person with ownership of that information, except as detailed in "Usage Monitoring" above.

Recovery of Information without user permission
The purposes for which individual information may sometimes be recovered and examined without the permission of the user include, but are not limited to:
- The restoration of deleted or inadvertently moved files.
- In performance management situations – e.g. where the nature and extent of a member's usage, communication, use of information, potential security breaches have given rise to concern and therefore need to be reviewed.
- Investigating the misuse of Hereworth ICT systems; determining the location of objectionable materials in personal folders or mailboxes/on cell-phones; obtaining evidence in regard to inappropriate communications or as part of internal disciplinary or criminal investigations.

Any recovered communications and/or information (including that of a personal nature) may be used in the associated investigation and inform any subsequent decision-making; such communications may also be removed, deleted or destroyed from Hereworth systems or workplaces.

Copyright and Intellectual Property Rights
If material subject to copyright is illegally copied to Hereworth systems, the organisation and the individual concerned may be liable. In all situations, copyright and intellectual property rights must therefore be protected; this relates, but is not limited to software and all programs, images, (video/film/photographs), sound recordings, applications, equipment, proprietary information and the attribution of authorship which must be respected.

The receiving, downloading, installing or copying of any unauthorised software/programs without the specific and formal (written) authorisation of Hereworth ICT is not permitted under any circumstances.

General Computer security

Every Hereworth computer (or mobile device) has an account allocated to either the individual user or specific station (or device) which allows access to the internet and / or email for the authorised user only. All access to the internet and email under an allocated individual will therefore be considered the responsibility of that individual.

If any email is received or an internet site (internal / external) is accessed that breaches this policy, the member concerned should advise their manager as soon as possible.

Members should log out or lock the system when leaving their computer terminal or mobile device for any length of time and ensure that messages sent from their system come directly from them or their appointed delegate(s).

Viruses

Members must exercise great care must when opening any attachment from unknown sources. All such attachments must be virus checked before downloading or opening. Any concerns or questions should be directed to a member of the ICT team.

Telephone security

Members have a responsibility to make responsible use of allocated landlines and/or Hereworth issued cell-phones as defined in this policy. Reviews of personal usage may be conducted as part of general system and usage management practices, including photographs, images, text and voicemail messages.

Social Media

Hereworth members are free to publish or comment via social media sites in accordance with this policy. Hereworth's rationale for this approach reflects its desire to create a dialogue between the organisation and its various markets/audiences as well as to engage potential markets/ audiences. It is recognised that the use of Social Media can have many positive effects for the organisation and will allow users to generate, communicate and share information at a low cost.

In recognising the inherent risks involved with the use of Social Media sites including, but not limited to:

- Damage to the reputation and brand of Hereworth.
- Loss of trust and confidence in Hereworth and its members.
- Loss of privacy.
- Loss in the control of organisational information, data & images.
- Identity fraud.
- Viruses.
- That any comments or articles posted within an online forum will remain there forever, even if deleted or removed once posted.

When making comments, or releasing information via a social platform, (either in an official or private capacity), members should therefore assess and adhere to the following principles:

S E L F:

Scrutiny

Will your comment withstand scrutiny by your colleagues, managers, media and members of the community?

Ethical

Is your comment ethical and consistent with Hereworth policies, procedures and processes? Does your post align with our Core Values?

Lawful

Is your comment lawful in regard to relevant legislation and Hereworth policies and procedures?

Fairness

Is your comment fair on Hereworth, your colleagues and the wider community?

How Hereworth members are expected to mitigate risks to the Organisation

To mitigate risks to all members of Hereworth, the use of Social Media must be used with care to avoid the following:

- Disclosure of information that breaches legislation and/or policies.
- Compromising the operational and strategic effectiveness of Hereworth by revealing either sensitive student or staff information or commercial activity.
- Compromising the trust, confidence, integrity and professionalism of Hereworth by expressing personal views that could be seen to represent the views of the organisation.
- Discrediting the organisation and/or any of its members through the depiction of inappropriate behaviour, particularly while in Hereworth uniform.

Approval to Set Up & Access Official Hereworth Social Media Profiles

Members wishing to establish a Hereworth social media profile for organisational purposes must adhere to all elements of this policy. Requests to establish should be made through the immediate manager to the Headmaster or Board Chairman and/or his delegate for approval.

Hereworth Branding/Visual Identity

Official Hereworth sites are those created in accordance with this policy which utilise the Hereworth name and/or branding. They are an entity through which the audience perceives themselves to be interacting directly with Hereworth.

All official Social Media Profiles once approved should be developed in collaboration with the Marketing Manager to ensure that the profile:

- Is consistent with Hereworth brand and values.
- Is consistent with the Hereworth website and other Hereworth publications.
- Displays official photographs and visual identity elements.
- Provides links back to the official Hereworth website to provide context and background while driving internet traffic via our main homepage.

Branding and organisational values information may be obtained from the Marketing Co-ordinator.

Official Hereworth photographs must be used for any profile photograph; they can be obtained from the Marketing Co-ordinator.

Users should also refer to the Hereworth Brand Guide available on the Hereworth Documents Drive, (Policies & Procedures, Procedures and Guidelines, Brand Guide) for further information and conventions on Hereworth Branding requirements.

Site Content:

Users must ensure Social Media conventions are observed, and that any commentary and criticism provided on the site is not inappropriate/ obscene/offensive. If offensive material is posted via a third party it must be removed immediately and the third party blocked from using the site.

Nothing is to be posted that could bring Hereworth into disrepute or conflict with organisational messages.

The Headmaster, Marketing Co-ordinator and delegated employees will be provided with administrator access to official social media sites to support high level monitoring and consistency with Hereworth policies and procedures.

Private Use of Social Media

Members of Hereworth have the same rights to free speech as other New Zealanders; however Hereworth membership in any capacity brings the additional responsibility of ensuring that the reputation and image of the organisation is not negatively impacted through the private use of social mediums.

In particular, members of Hereworth must:

- Ensure any comments and/or contributions on a social media site are clearly identified as personal and it is clear that they do not represent the view of the organisation.
- Not display images or participate in any conversation that may damage the trust and confidence the public has in Hereworth.
- Not display the Hereworth uniform including signage and insignia without prior approval.
- Not disclose any information they do not have the authority to disclose.
- Not make derogatory or offensive remarks and/or comments directed at Hereworth or any member of Hereworth or external stakeholders.

Online Security

The majority of Social Media sites allow for user pages to be 'locked down' which only allows access to a select group of users. With the exception of Social Media sites used for community engagement and promotional purposes, users should attempt to make their sites as secure as possible from the risk of profiles being hacked or infiltrated.

Review

This policy shall be reviewed every two years or more regularly by agreement.
The provisions of this agreement may be varied by the Board following consultation with staff.

Signatures

Signed: _____ Date: ____/____/____