Te Kura
Te Aho o Te Kura Pounamu

Hātepe Kaimahi

What guides us

Living Te Tiriti o Waitangi
Ensuring ākonga are at the centre of everything we do
Delivering high-quality, future-focused teaching and learning

Poipoi – Kauawhi – Tāuteute – Pūnaha Auaha – Ārahi
Nurture – Include – Engage – Innovate – Lead

RESPONSIBLE ICT USE

Date of approval	: 31/1/2025
Date first created/This version no.	: 2025/1
Next review date (3 year cycle)	: 2028
Sponsor	: Deputy Chief Executive Systems and Support
Owner	: Chief Information Officer
Who are these procedures for	: All kaimahi and ākonga

This hātepe supports the Kaimahi Code of Conduct approved by the Board of Trustees.

Scope and purpose

1. This hātepe provides direction to Te Aho o Te Kura Pounamu (Te Kura) Users about the acceptable use of ICT.
2. This hātepe applies to all Te Kura ICT and any personal devices connecting to or using Te Kura systems and services.
3. This hātepe applies to all Te Kura technology Users as defined.
4. Everyone covered by this hātepe, regardless of their position, must always comply with New Zealand laws and this hātepe.

Delegated authorities

5. Any decision to incur ICT costs or make financial commitments must comply with the Financial and Human Resources Delegations Governance Policy.

Definitions

Term	Definition
Core ICT	Include, but are not limited to, Student Information Systems and related (Student Management Systems, Onboarding Systems, Registration Systems, Student Support Systems), Learning Management Systems (LMS), Human Resources Management Information Systems (HRMIS), Financial Management Information Systems (FMIS), and Electronic Management Systems (EDRMS).
Cyber Safety Incident	Any event that threatens the confidentiality, integrity, or availability of digital information, technology systems, identities or networks of Te Kura. This includes, but is not limited to, unauthorised access, data breaches, malware attacks, and phishing attempts. Such incidents can compromise the security of sensitive data, disrupt services, or put the assets and reputation of Te Kura at risk.
File Sharing	Uploading and downloading material from the Internet, using an application, service or network that enables simultaneous sharing of material between multiple

Term	Definition
	users. It includes, for example, downloading media, movies, music, e-books and computer software.
ICT	ICT may include, but is not limited to, computers (such as desktops, laptops, and tablets), computer systems, storage devices, cameras (such as video, digital, webcams), mobile phones, video and audio players/receivers and telecommunication equipment, networks, software, cloud services, databases and any other similar technologies as they come into use.
Information Resources Group (IRG)	IRG support and maintain the school's ICT strategy, telecommunications and records management to assist the school in achieving its objectives.
Kaimahi	A staff member, including permanent, fixed-term, temporary, and seconded employees, as well as volunteers and contractors engaged by Te Kura, regardless of whether they work full-time, part-time, or casually. For the purposes of this document, Kaimahi refers to all these individuals.
Personal Device	Any ICT owned or provided by a User, rather than provided by Te Kura, that can be used for communication, information storage, access, or processing. Examples include phones, tablets, laptops, wearable technology (like smartwatches), and any other privately-owned digital devices capable of connecting to networks or storing data.
Use of ICT Agreement	Outlines the expectations, and responsibilities Users Te Kura ICT resources. Refer Use of ICT Agreement – Kaimahi and ākonga process.
User	Kaimahi, ākonga, or any individual authorised to access or use Te Kura ICT.
Frequently used terms, including Te Reo Māori, can be found here.	

Procedure

Objectives

6. Te Kura is committed to fostering safe and responsible ICT use by:
    a. Promoting awareness among all Users about the appropriate use of ICT, in alignment with the purpose, values, and goals of Te Kura.
    b. Supporting digital citizenship, ensuring every ākonga can achieve their highest possible educational standard.
    c. Encouraging a culture of transparency where users and those engaged with Te Kura feel empowered to raise any concerns regarding ICT use in a responsible, constructive way.

Requirements when using Te Kura ICT

7. To access Te Kura ICT, Users must sign and return the relevant Responsible ICT Use Agreement.
8. All users are expected to use Te Kura's ICT for educational or school administration related tasks, consistent with their conditions of enrolment or conditions of employment.
9. Users must avoid any actions that may damage, slow down, or interfere with Te Kura systems, stored data, or information. Users must not attempt to access information or systems for which they do not have authorisation.

Connecting to personal or public network or personal phone

10. Public networks can be insecure, potentially exposing users to threats like hacking, malware, or data interception. Personal devices may also have lower security measures than the Te Kura network.
11. Kaimahi must not store Te Kura records on Personal Devices or unauthorised networks. When connecting Te Kura ICT to Personal Devices or public networks, users must prioritise security measures to protect sensitive data.

Accountability for your User account

12. Users are accountable for any activity carried out under their account. They must ensure that access remains secure and must not be shared with others.

Passwords and security

13. Users are responsible for safeguarding their passwords and other security credentials. Passwords and other security credentials must not be shared with others.
14. If a password becomes compromised or potentially insecure, the user must report it to IRG Service Desk immediately and change their password as soon as possible.

Compliance with Official Information Act and privacy requirements

15. All data and information stored on the ICT systems of Te Kura, as well as well as any Te Kura data stored outside these systems, is subject to requirements under the Official Information Act, Privacy Act, and Records Act. This includes all electronic communications such as emails, texts, direct messages, and recordings (e.g., Teams sessions, or other messaging applications).
16. When creating records, users must ensure the content is appropriate and does not risk harm to Te Kura's or the public sector's reputation if released publicly or to individuals.
17. Users must also consider security classifications and any relevant Privacy Governance Policy requirements when handling, viewing, or sharing records.

Copyright and licensing

18. Users must comply with all applicable licences when using printed, electronic, video, and audio materials. Copying, altering, or sharing third-party content must strictly follow licensing terms and New Zealand copyright laws, including the Copyright Act 1994 and related amendments – refer to Intellectual Property, Copyright, and Other Related Rights Governance Policy.

Prohibited activities

19. All Users must comply with New Zealand Law and Regulations regarding privacy, defamation, objectionable material, and human rights. Users must also not engage in any prohibited activities, including accessing, storing, viewing, or sharing content that is:
    a. Pornographic in nature.
    b. Defamatory, offensive, fraudulent, threatening, harassing, or illegal.
    c. Promoting the personal, cultural, commercial, political, or religious interests of the User, their whānau or friends.
    d. Software, media, or data unlawfully obtained (illegal File Sharing).
    e. Excessive in volume, such as chain emails, or subscriptions to services unrelated the business or educational objectives of Te Kura.
    f. Is likely to harm the reputation of Te Kura or the public service.

Limited personal use

20. Limited personal use of the ICT resources of Te Kura is permitted, provided it remains reasonable and appropriate, does not interfere with school activities, and does not result in additional costs or misuse of public resources.

21. Personal use must not pose a risk to the reputation or security of Te Kura. The following activities are not permitted:

    a. Gambling, gaming, and streaming movies.
    b. Installing or using apps, software, or online services not authorised by Te Kura.
    c. Using a Te Kura email or other accounts for personal matters.
    d. Engaging in private business or commercial activities.

Internet use and social media

22. Internet use is intended for educational and school administration purposes, with limited personal use if it is appropriate in a school setting. Te Kura conducts regular audits of sites visited by users and maintains blocks for web content that it considers inappropriate or that may pose a risk to the reputation or security of Te Kura.

23. When using social media Users must comply with the [Use of Social Media Hātepe Kaimahi].

Reporting Cyber Security Incidents

24. Users must report any suspected security breaches or unauthorised use of ICT immediately – refer to **Appendix A**.

25. Cyber Security Incident management must align with the Ministry of Education Digital Technology: Safe and responsible use in schools guidelines.

Monitoring and investigation

26. Authorised individuals and automated systems within Te Kura monitor technology and network traffic, which may include User created traffic, for security and network maintenance purposes.

27. Te Kura reserves the right to audit user activity, networks, and systems for security and network maintenance purposes and to ensure compliance with this hātepe. Te Kura may obtain and use any data or information generated or accessed through it and report this accordingly to management.

28. Te Kura may without notice delete any non-work related content or impose restrictions on technology, including access, not serving legitimate business or educational purpose.

29. Te Kura may exclude a User from the information systems pending investigation of the alleged breach.

Conflict of interest

30. A conflict of interest occurs when a Kaimahi has a private or personal interest that could benefit, or seem to benefit, from their professional decisions or actions within Te Kura.

31. If you become aware of a potential conflict of interest, you must report it following the procedures outlined in the [Conflict of Interest Hātepe Kaimahi].

Fraud

32. If you suspect that a fraudulent act may be occurring or may have occurred, you must report this immediately in accordance with the Fraud Reporting & Investigation Hātepe Kaimahi.

Compliance

33. Alleged breaches of this hātepe may be treated as misconduct or serious misconduct and managed in accordance with the Kaimahi Code of Conduct of Te Kura and any applicable employment agreement.

Key accountabilities and responsibilities

Role	Description of responsibility
Chief Executive	Responsible for: • approval of this hātepe. • Te Kura meeting its obligations under this hātepe. • ensuring any breaches of this hātepe have been addressed.
Chief Advisor, Strategy	Responsible for: • ensuring the owners of this hātepe regularly review and meet Te Kura's current standards.
Deputy Chief Executives (DCEs)	Responsible for: • embedding this hātepe in their wāhanga. • ensuring their wāhanga are compliant with this hātepe.
Hātepe Owner	Responsible for: • ensuring the hātepe is working effectively through regular monitoring and reporting of compliance with the hātepe. • ensuring Kaimahi have had the opportunity to receive training on this hātepe, where required. • ensuring any breaches of this hātepe have been addressed.
Kainga Managers	Responsible for ensuring the proposed expenditure, decision, or activity: • is necessary and reasonable, for Te Kura purposes. • is considered financially prudent and will withstand public scrutiny. • has been approved consistent with the Financial and Human Resources Delegations Governance Policy. • is consistent with all Te Kura policies. • is covered by the available budget prior to requesting approval. • is supported by the appropriate documentation and is correctly coded.
All Kaimahi	Responsible for: • complying with this and all other relevant Te Kura policies. • reporting any non-compliance with this hātepe to their manager.

Monitoring and assurance

34. The Hātepe Owner has the overall responsibility for monitoring the hātepe for effectiveness and compliance.

Measures of success

35. The hātepe will be considered effective if:

    a. Hātepe users' feedback on appropriateness and ease of application is positive.

b. Reporting is complete and accurate.
c. There are no breaches of the hātepe, or if there are breaches, they are dealt with in a timely and appropriate manner.

Compliance management

36. Compliance management tools and processes will be used to ensure compliance with this hātepe. The tools and processes may include:
    a. Monitoring of compliance with required processes, procedures or guidelines as set out in this hātepe and related procedures.
    b. Spot checks conducted by the Hātepe Owner on a regular basis to ensure compliance.
    c. Key messages will be provided to the business where spot checks have identified non-compliance.
    d. Tools such as checklists or online modules to help inform Kaimahi of their relevant obligations.

Reporting and information

37. The Hātepe Owner will report to the Risk & Assurance Committee in accordance with the annual assurance plan.

Further support and guidance

38. Additional information that supports this hātepe can be found in:
    a. [Anti-Bullying, Anti-Harassment and Anti-Discrimination Hātepe Kaimahi]
    b. Kaimahi Code of Conduct
    c. Conflict of Interest Governance Policy
    d. Financial and Human Resources Delegations Governance Policy
    e. Fraud Prevention and Detection Governance Policy
    f. Information and Records Management Hātepe Kaimahi
    g. Intellectual Property, Copyright, and Other Related Rights Governance Policy
    h. Policy Framework Governance Policy
    i. Kaimahi Privacy Statement
    j. [Use of Social Media Hātepe Kaimahi]
    k. Digital Technology: Safe and responsible use in schools (Ministry of Education)
    l. Copyright Act 1994
    m. Copyright (Infringing File Sharing) Amendment Act 2011
    n. Defamation Act 1992
    o. Education and Training Act 2020
    p. Harmful Digital Communication Act 2015
    q. Human Rights Act 1993
    r. Official Information Act 1982
    s. Privacy Act 2020
    t. Protected Disclosures (Protection of Whistleblowers) Act 2022
    u. Public Records Act 2005
    v. Trade Marks Act 2002
    w. Unsolicited Electronic Messages Act 2007

Approved by Te Rina Leonard, Chief Executive, Te Aho o Te Kura Pounamu

Appendix A: Procedures for reporting Cyber Security Incidents

1. Prompt identification, reporting, and response to Cyber Security Incidents is important to minimise potential harm and to protect Users and Te Kura.

Procedures for self-reported incidents

2. Any User who encounters any image or material deemed inappropriate or contrary to this hātepe or any other related Te Kura policy must promptly report the incident.
3. The User should avoid opening email attachments, following URL links, or viewing thumbnail images if there is a suspicion that the material is inappropriate. If the image or website has already been accessed, the application must remain open without forwarding or printing anything, as any action could compromise evidence and impede further investigation.
4. The user must log a service desk request regarding the incident with the IRG Service Desk through the intranet or via phone. Upon receiving the report, the IRG Service Desk will record it as a Cyber Safety Incident, issue a call number, and communicate this to the user. The call number will be retained by the IRG in case it is needed during a future computer audit.
5. The user will complete and sign a Cyber Safety Incident Form, providing details of the incident and their actions. They must then notify their immediate manage, who also signs the form. The user should retain the form until they are contacted by an IRG cyber safety support person.
6. The IRG cyber safety support person will contact the User within 30 minutes of receiving the request, review the relevant images or material, confirm their location, and arrange to collect the signed Cyber Safety Incident form, either in person or through electronic means as agreed with the user.
7. The IRG cyber safety support person will then review the incident with the Chief Information Officer (or their delegate) to assess its significance using Department of Internal Affairs ratings for illegal or objectionable material, and to determine if a forensic assessment of the User's device is necessary. Consideration will also be given to whether the incident could reasonably be explained as accidental, based on the User's description, and what follow-up actions should be taken, ranging from recording and removing the material to escalating the matter to a Senior Leadership Team (SLT) member for further investigation or an external audit.
8. All actions taken during the incident review will be documented on the Cyber Safety Incident Form. Once the incident is closed, the IRG will update the cyber safety register and file a copy of the Cyber Safety Incident Form with Human Resources (HR).
9. Te Kura is committed to applying the principles of natural justice throughout the investigation process, including protecting the privacy of those involved as much as practicable and in line with the Privacy Act 1993.

Procedures for observed incidents

10. If a User observes any potential breach of this hātepe or any other related Te Kura policy, regardless of whether it appears intentional, they must report the incident. The observer will immediately notify their manager or a relevant SLT member, who will then complete a Cyber Safety Incident Form with the observer and inform the Chief Executive (CE) and the Chief Information Officer.
11. The Chief Information Officer will record the incident as 'observed' Cyber Safety Incident, assign a call number, and advises this to both the SLT member and the observer.

12. Should there be sufficient evidence, the involved User will be approached promptly and asked to surrender their Te Kura ICT device for an independent external audit. If evidence is lacking or inconclusive, the device will be scheduled for auditing outside of work hours as soon as feasible. The incident will then be subject to formal investigation.
13. Throughout all stages, Te Kura will uphold the principles of natural justice, maintaining the privacy of all parties involved whenever possible in accordance with the Privacy Act 1993. Actions taken during the investigation will be fully documented, and, upon closure, the cyber safety register will be updated, and a copy of the incident form will be filed with HR.

Procedures for Incidents Identified in Management Reports

14. Te Kura continuously monitors and manages the appropriate use of internet and email technology. The IRG generates various ICT usage reports, including but not limited to lists of the top users accessing adult or blocked sites, uncategorized sites, and highest email usage.
15. If a manager deems that a report provides sufficient evidence of a Cyber Safety Incident or finds an unsatisfactory explanation for reported ICT activity, they will determine if the situation warrants formal disciplinary proceedings. In such cases, the procedures outlined for observed incidents are followed, and any evidence on the User's equipment is preserved.
16. The Deputy Chief Executive Systems & Support will inform the Board of any significant ICT issues requiring attention.