Ngā Tikanga Hāpai i te Hangarau Pārongo

ICT Acceptable Use Policy

1. Introduction

1.1 The Electoral Commission's ICT (Information Communication Technology) Acceptable Use Policy defines clear responsibilities and expectations for safe, secure and appropriate use of ICT within the Electoral Commission.

1.2 This policy highlights standard obligations expected to protect and safeguard the Electoral Commission from risk, compromised reputation and/or prosecution under New Zealand legislation related to the use of computers, software, internet, email, and any other ICT resources.

1.3 This policy also details how it is enforced with comprehensive system monitoring, as well as actions that may be taken in the event this policy is breached.

1.4 The ICT Acceptable Use Policy supports our strategic objectives and aligns with our values, Poutokomanawa. For more details, see Poutokomanawa - our values | ECHO

2. Scope

2.1 This policy applies to all employees, contractors, secondees, and consultants who work for or at the Electoral Commission, referred to as 'kaimahi' throughout the policy.

3. Policy

Acceptable use of ICT systems

3.1 Commission ICT systems are provided to kaimahi for Commission-related business use, which is considered as:

- completing tasks that are cited in the job description of the kaimahi
- completing tasks that are cited in Commission process documentation or guides
- any other use that has been authorised by the manager of the kaimahi.

3.2 Occasional web browsing to public internet websites for personal use is permitted if it meets the criteria below.

- Personal use does not impede kaimahi work output or quality.
- Daily personal use of ICT is not excessive. For example, actively browsing social media for multiple hours would be considered excessive personal use.
- Personal use does not consume any Commission resources or IT support or create any undue costs.
- No potentially malicious file types are downloaded to a Commission device. This includes file types that run code, such as executables, scripts, macros, installers and others. Other file types such as documents or images may be downloaded.
- Personal use does not put the reputation or information security of the Commission at risk or impede any business processes.
- Personal use is reasonable to consider as 'safe for work' and does not breach any Commission policy including other clauses of this policy.

All other use is not permitted as it may put the Commission at risk.

Examples of personal use that is considered acceptable are browsing news websites, using approved social media, checking personal email, listening to background audio, booking things such as travel or accommodation.

Personal use of ICT is also subject to the Monitoring and Auditing of ICT systems use described in this policy.

3.3 Commission ICT systems and equipment/devices are to be used only by kaimahi that have been explicitly provided access to the system. Kaimahi must not provide access (login for someone) or share credentials (such as passwords) to anyone else or use any access that is not explicitly intended for their own use under any circumstances. This also includes sharing credentials with any colleagues, IT support kaimahi or third-party vendors.

3.4 Due diligence is taken to uphold cyber security at the Commission, and the Cyber Security Policy is adhered to. Actions that put the Commission at risk are avoided. Common examples are listed below.

- Downloading unapproved software from the internet (such as, applications, browser extensions, scripts, or macros).
- Reckless/negligent or intentional access of malicious websites and other content.
- Allowing other people to use your device or accounts or using someone else's device or accounts.
- Not taking reasonable care to identify and report cyber-attacks, such as phishing emails.
- Not keeping your laptop or other devices physically safe, for example leaving them in an insecure location where they may be stolen, lost, or accessed by someone who is not authorised.
- Using or submitting Commission information to an unapproved online service. For example, DropBox for file sharing, an online PDF editor, ChatGPT, or sending Commission-related emails using other email services such as Gmail, unless specifically approved by the Chief Information Officer.

3.5 Deliberately subverting ICT systems, processes, and security mechanisms is unacceptable use of ICT. Possible examples of this type of activity may be attempting to or successfully:

- tampering with security software or system configurations
- deviating from standard business processes to bypass security controls.

3.6 Care is taken to ensure information is stored in appropriate and secure locations. Private, sensitive, and confidential information is stored in approved locations that are only accessible to people that have the right to access the information. For example, Microsoft Teams is an appropriate and secure location to store information if it is placed in the correct Team with the appropriate access settings.

3.7 No Commission data or information is to be sent outside of the Commission unless for legitimate work purposes. For example, Commission data or information should not be sent to personal e-mail addresses of Commission kaimahi except for legitimate communications such as employment information.

3.8 Using Commission business information or applications that hold sensitive or private information for personal use, personal gain, or any use other than the explicit purpose intended is unacceptable use of ICT.

3.9 Inappropriate or 'not safe for work' use of Commission systems is not permitted. Inappropriate use includes but is not limited to:

- taking part in any illegal activities

- disclosing confidential information to unauthorised parties
- the blatant misuse or mistreatment of IT assets
- any profit-related activity or conducting any personal commercial activities
- soliciting for personal gain
- seeking to gain unauthorised access to systems or information or attempting to bypass security controls
- knowingly altering the integrity of any information with malicious or dishonest intent
- deliberate downloading, retaining, transmitting, or viewing of:
  - pornography or any vulgar material
  - profane material
  - insulting material
  - blatantly offensive material
  - material of a sexual nature
- downloading any software from a non-approved source, such as through a browser
- playing any online games or gambling
- making indecent remarks or conducting electronic harassment/bullying of any kind
- defamation of any individual or organisation
- passing personal views off as those of the Commission
- any actions or communication that are not considered politically neutral and impartial
- intentionally creating a security breach or disruption of technology
- displaying sensitive information in public places.

3.10 All kaimahi must follow any Commission guidance relating to emerging and new technology. As an example, the Commission does not currently allow the use of generative artificial intelligence (AI) for work purposes, unless the use is approved by the Chief Information Officer. If you are in doubt about what emerging technologies are approved for work purposes, including AI, talk to your manager or contact IT.

Authority to control ICT systems

3.11 All data and information stored on, and transmitted to and from, the Commission's ICT systems are considered the property of the Commission.

3.12 While the Commission respects the privacy of kaimahi by avoiding access to personal or private information described in section 3.2, it reserves the right to access such information under specific circumstances. These circumstances include, but are not limited to, security investigations or inquiries into alleged breaches of conduct.

3.13 The Commission treats all information transmitted through or stored on any of our Electoral Commission systems, including email messages, as Commission business information and is subject to scrutiny by the Commission. All information on Electoral Commission ICT systems may be subject to Official Information Act (OIA) requests.

3.14 The Commission reserves the right to control, configure, and restrict any use of ICT systems to secure information and ICT systems, enforce ICT policies, or to implement any other business requirements.

3.15 These clauses also apply to Commission-owned or provided online services. For example, Microsoft 365 used from a computer that is not owned by the Commission, such as a personally owned device.

Monitoring and Auditing of ICT systems use

3.16 The Electoral Commission will adopt at any time any number of methods to monitor, log, audit, and apply information security controls to, the use of all Commission ICT systems and information to ensure compliance with the ICT Acceptable Use Policy.

3.17 To ensure compliance with this and other policies, all use of the Electoral Commission ICT systems is monitored. Detailed logs of all system use, including personal use, are recorded and stored and any other information, such as communications or documents, may be audited. This information is handled in accordance with the Privacy Act 2020. Information produced by monitoring and auditing of Commission ICT systems may be used in investigations and as evidence of a policy being breached.

Consequence for non-compliance

In the event of breaches to policy clauses, the Commission may take appropriate actions. For example:

- The manager of the kaimahi may be advised of the policy breach.
- Disciplinary action may be taken in cases of breaches or misconduct.
- Detailed analysis of information captured and held by the Commission may be undertaken.
- Access may be revoked or limited to any ICT systems or devices.
- Any violations considered potentially illegal may be reported to appropriate authorities.

4. Responsibilities

Managers

4.1 Managers are responsible for ensuring that kaimahi, contractors, secondees, and consultants understand their responsibilities under this policy in relation to ICT acceptable use.

All kaimahi

4.2 Each kaimahi is accountable for their own behaviour in respect of meeting the obligations of this policy and is responsible for ensuring the Electoral Commission standards are not breached.

4.3 If an employee is unsure of any aspect of this policy, or requires any clarification, they are responsible for seeking help from their manager or the ICT support team.

5. Related Policies, Procedures, Legislation

Related policies

- Managing Employee Conduct and Performance
- Intranet Procedures
- Code of Conduct
- Data and Information Management Policy
- Personal Information & Privacy Act Policy
- Cyber Security Policy
- Workplace Behaviour Policy

Legislation

- Public Records Act 2005
- Copyright Act 1994
- Employment Relations Act 2000
- Health and Safety at Work 2015
- Human Rights Act 1993
- Official Information Act 1982
- Privacy Act 2020.

6. Definitions

6.1 Terms used in this policy are defined below.

Term	Definition
Kaimahi	Te reo Māori word meaning worker or employee.
Information Communication Technology (ICT)	Refers to technologies that enable the access, creation, and exchange of information through digital means.
Logs	Records of events and actions that occur in a system.
Software	Any computer program or application.
Cyber attack	A malicious attack against Commission ICT systems.
Phishing	A common technique to carry out a cyber attack by contacting kaimahi in an attempt to manipulate them into exposing information or completing risky actions.
Generative Artificial Intelligence	A type of artificial intelligence that can produce various types of content, including text, imagery, audio and synthetic data. Common examples are CoPilot and ChatGPT.

7. Policy status and approval

Version	September 2025 (minor amendments)
Approval authority	Board
Approval date	December 2024
Policy owner	DCE, Enterprise Services
Revision cycle	3 yearly
Next review	September 2028

Ngā Tikanga Hāpai i te Hangarau Pārongo
ICT Acceptable Use Policy

1. Introduction

1.1 The Electoral Commission's ICT (Information Communication Technology) Acceptable Use Policy defines clear responsibilities and expectations for safe, secure and appropriate use of ICT within the Electoral Commission.

1.2 This policy highlights standard obligations expected to protect and safeguard the Electoral Commission from risk, compromised reputation and/or prosecution under New Zealand legislation related to the use of computers, software, internet, email, and any other ICT resources.

1.3 This policy also details how it is enforced with comprehensive system monitoring, as well as actions that may be taken in the event this policy is breached.

1.4 The ICT Acceptable Use Policy supports our strategic objectives and aligns with our values, Poutokomanawa. For more details, see Poutokomanawa - our values | Ruawhetū

2. Scope

2.1 This policy applies to all employees, contractors, secondees, and consultants who work for or at the Electoral Commission, referred to as 'kaimahi' throughout the policy.

3. Policy

Acceptable use of ICT systems

3.1 Commission ICT systems are provided to kaimahi for Commission-related business use, which is considered as:

- completing tasks that are cited in the job description of the kaimahi.
- completing tasks that are cited in Commission process documentation or guides.
- any other use that has been authorised by the manager of the kaimahi.

3.2 Occasional web browsing to public internet websites for personal use is permitted if it meets the criteria below.

- Personal use does not impede kaimahi work output or quality.
- Daily personal use of ICT is not excessive. For example, actively browsing social media for multiple hours would be considered excessive personal use.
- Personal use does not consume any Commission resources or IT support or create any undue costs.
- No potentially malicious file types are downloaded to a Commission device. This includes file types that run code, such as executables, scripts, macros, installers and others. Other file types such as documents or images may be downloaded.
- Personal use does not put the reputation or information security of the Commission at risk or impede any business processes.
- Personal use is reasonable to consider as 'safe for work' and does not breach any Commission policy including other clauses of this policy.

All other use is not permitted as it may put the Commission at risk.

Examples of personal use that is considered acceptable are browsing news websites, using approved social media, checking personal email, listening to background audio, booking things such as travel or accommodation.

Personal use of ICT is also subject to the Monitoring and Auditing of ICT systems use described in this policy.

3.3 Commission ICT systems and equipment/devices are to be used only by kaimahi that have been explicitly provided access to the system. Kaimahi must not provide access (login for someone) or share credentials (such as passwords) to anyone else or use any access that is not explicitly intended for their own use under any circumstances. This also includes sharing credentials with any colleagues, IT support kaimahi or third-party vendors.

3.4 Access for Kaimahi to commission systems is restricted to New Zealand unless approved in advance by following the 'requesting to work from overseas' process or explicit approval for work purposes

3.5 Due diligence is taken to uphold cyber security at the Commission, and the Cyber Security Policy is adhered to. Actions that put the Commission at risk are avoided. Common examples are listed below.

- Downloading unapproved software from the internet (such as, applications, browser extensions, scripts, or macros).
- Reckless/negligent or intentional access of malicious websites and other content.
- Allowing other people to use your device or accounts or using someone else's device or accounts.
- Not taking reasonable care to identify and report cyber-attacks, such as phishing emails.
- Not keeping your laptop or other devices physically safe, for example leaving them in an insecure location where they may be stolen, lost, or accessed by someone who is not authorised. This includes ensuring that devices are carried as hand luggage when travelling.
- Using or submitting Commission information to an unapproved online service. For example, DropBox for file sharing, an online PDF editor, ChatGPT, or sending Commission-related emails using other email services such as Gmail, unless specifically approved by the Chief Information Officer.
- Using unauthorised instant messaging software.

3.6 Kaimahi who receive what they believe to be a virus or any other malicious software must immediately call the Service Desk or advise IT Security in person.

3.7 Deliberately subverting ICT systems, processes, and security mechanisms is unacceptable use of ICT. Possible examples of this type of activity may be attempting to or successfully:

- tampering with security software or system configurations.
- deviating from standard business processes to bypass security controls.

3.8 Care is taken to ensure information is stored in appropriate and secure locations. Private, sensitive, and confidential information is stored in approved locations that are only accessible to people that have the right to access the information. For example, Microsoft Teams is an appropriate and secure location to store information if it is placed in the correct Team with the appropriate access settings.

3.9 No Commission data or information is to be sent outside of the Commission unless for legitimate work purposes. For example, Commission data or information should not be sent to personal e-mail addresses of Commission kaimahi except for legitimate communications such as employment information.

3.10 Commission workstations must also be screened locked when not in use and internal and confidential information should not be visible on a screen where unauthorised users can view this information.

3.11 Kaimahi are responsible for the safety of their passwords and PINs for commission ICT systems. They must:

- Be kept confidential.
- Not be written down – Kaimahi can use the Commission approved password manager to store and manage passwords. This is available in your EDGE browser.
- Changed whenever there is any indication of possible system or password compromise
- Laptop passwords and PINs must be a minimum of 8 characters long. They must be long, strong and unique.
- Mobile phone PINs must be 6 characters long.

3.12 Using Commission business information or applications that hold sensitive or private information for personal use, personal gain, or any use other than the explicit purpose intended is unacceptable use of ICT.

3.13 Inappropriate or 'not safe for work' use of Commission systems is not permitted. Inappropriate use includes but is not limited to:

- taking part in any illegal activities.
- disclosing confidential information to unauthorised parties.
- the misuse or mistreatment of IT assets.
- any profit-related activity or conducting any personal commercial activities.
- soliciting for personal gain.
- seeking to gain unauthorised access to systems or information or attempting to bypass security controls.
- knowingly altering the integrity of any information with malicious or dishonest intent.
- deliberate downloading, retaining, transmitting, or viewing of:
  - pornography or any vulgar material
  - profane material
  - insulting material
  - blatantly offensive material
  - material of a sexual nature
- downloading any software from a non-approved source, such as through a browser.
- playing any online games or gambling.
- making indecent remarks or conducting electronic harassment/bullying of any kind.
- defamation of any individual or organisation.
- passing personal views off as those of the Commission.
- any actions or communication that are not considered politically neutral and impartial.
- intentionally creating a security breach or disruption of technology.
- displaying sensitive information in public places.

3.14 All kaimahi must follow any Commission guidance relating to emerging and new technology. As an example, the Commission does not currently allow the use of generative artificial intelligence (AI) for work purposes, unless the use is approved by the Chief Information Officer. If you are in doubt about what emerging technologies are approved for work purposes, including AI, talk to your manager or contact IT.

Authority to control ICT systems

3.15 All data and information stored on, and transmitted to and from, the Commission's ICT systems are considered the property of the Commission.

3.16 While the Commission respects the privacy of kaimahi by avoiding access to personal or private information described in section 3.2, it reserves the right to access such information under specific circumstances. These circumstances include, but are not limited to, security investigations or inquiries into alleged breaches of conduct.

3.17 The Commission treats all information transmitted through or stored on any of our Electoral Commission systems, including email messages, as Commission business information and is subject to scrutiny by the Commission. All information on Electoral Commission ICT systems may be subject to Official Information Act (OIA) requests.

3.18 The Commission reserves the right to control, configure, and restrict any use of ICT systems to secure information and ICT systems, enforce ICT policies, or to implement any other business requirements.

3.19 These clauses also apply to Commission-owned or provided online services. For example, Microsoft 365 used from a computer that is not owned by the Commission, such as a personally owned device.

Monitoring and Auditing of ICT systems use

3.20 The Electoral Commission will adopt at any time any number of methods to monitor, log, audit, and apply information security controls to, the use of all Commission ICT systems and information to ensure compliance with the ICT Acceptable Use Policy.

3.21 To ensure compliance with this and other policies, all use of the Electoral Commission ICT systems is monitored. Detailed logs of all system use, including personal use, are recorded and stored and any other information, such as communications or documents, may be audited. This information is handled in accordance with the Privacy Act 2020. Information produced by monitoring and auditing of Commission ICT systems may be used in investigations and as evidence of a policy being breached.

Consequence for non-compliance

3.22 In the event of breaches to policy clauses, the Commission may take appropriate actions. For example:

- The manager of the kaimahi may be advised of the policy breach.
- Disciplinary action may be taken in cases of breaches or misconduct.
- Detailed analysis of information captured and held by the Commission may be undertaken.
- Access may be revoked or limited to any ICT systems or devices.
- Any violations considered potentially illegal may be reported to appropriate authorities.

4. Responsibilities

Managers

4.1 Managers are responsible for ensuring that kaimahi, contractors, secondees, and consultants understand their responsibilities under this policy in relation to ICT acceptable use.

All kaimahi

4.2 Each kaimahi is accountable for their own behaviour in respect of meeting the obligations of this policy and is responsible for ensuring the Electoral Commission standards are not breached.

4.3 If an employee is unsure of any aspect of this policy, or requires any clarification, they are responsible for seeking help from their manager or the ICT support team.

5. Related Policies, Procedures, Legislation

Related policies

- Managing Employee Conduct and Performance
- Intranet Procedures
- Code of Conduct
- Data and Information Management Policy
- Personal Information & Privacy Act Policy
- Cyber Security Policy
- Workplace Behaviour Policy

Legislation

- Public Records Act 2005
- Copyright Act 1994
- Employment Relations Act 2000
- Health and Safety at Work 2015
- Human Rights Act 1993
- Official Information Act 1982
- Privacy Act 2020.

6. Definitions

6.1 Terms used in this policy are defined below.

Term	Definition
Kaimahi	Te reo Māori word meaning worker or employee.
Information Communication Technology (ICT)	Refers to technologies that enable the access, creation, and exchange of information through digital means.
Logs	Records of events and actions that occur in a system.
Software	Any computer program or application.
Cyber attack	A malicious attack against Commission ICT systems.
Phishing	A common technique to carry out a cyber attack by contacting kaimahi in an attempt to manipulate them into exposing information or completing risky actions.
Generative Artificial Intelligence	A type of artificial intelligence that can produce various types of content, including text, imagery, audio and synthetic data. Common examples are CoPilot and ChatGPT.

7. Policy status and approval

Version	January 2026 (minor amendments)
Approval authority	Board
Approval date	February 2026
Policy owner	DCE, Enterprise Services
Revision cycle	3 yearly
Next review	February 2029