Document 1

Technology and facilities Calling, meeting room & conferencing technology Virtual Meeting Rooms (Teams) Microsoft Teams

Microsoft Teams

Microsoft Teams is the Ministry's primary application for internal calls and both internal and external meetings.

Teams is a place for your team to chat, meet, plan and share information. Using Teams will help you collaborate and communicate more seamlessly with your colleagues in a single application and hopefully reduce your emails!

Participate in a continuous group conversation with people you work with. Have a conversation right where the work is happening, whether co-authoring a document in real time, having a meeting, or working together in other apps and services. Teams is the place to iterate quickly on a project, work with team files, and collaborate on shared deliverables.

Select the link below to watch a video on Microsoft collabration tools. The video opens in a new page.

Microsoft 365 - Video suite (education.govt.nz)

M365 Hub

The M365 Hub is where you can find all types of information, training and tips on Teams (as well as other M365 applications like OneDrive)

Useful Microsoft Teams resources:

- *When to use Teams and when to use Skype*
- *Microsoft Teams **FAQs***
- *Microsoft Teams **Top Tips***
- *Managing **Notifications** in Teams*
- *Running Effective **Meetings***

Teams meeting types & features

Meeting Method> **Feature**	**Teams Meeting**	**Teams Webinar**	**Teams Live Event**

Scenario	Meetings are great for scheduled or impromptu interactions and collaboration with smaller audiences. They provide no ability to choose how you want participants to engage.	Webinars are ideal for presentation event needs, where ad-hoc audience interactions are required. They allow you to choose how you want participants to engage and include controls which provide more options, enhancing user experience. Webinars also provide some helpful richer functionality over Teams live events (such as the ability to use breakout rooms etc)	A live event should be used for broadcast purposes to large audiences only. It has no audience interaction capabilities beyond Q&A functionality.
Number of Attendees	Up to 1000 (up to 20,000)	Up to 1000 (Overflow attendees beyond the 1,000 limit join in view-only mode, up to 10,000) (currently overflow limit of 20,000 until end of 2021 due to COVID)	Up to 10,000 (currently 20,000 until end of 2021 due to COVID) Additionally, Live Events with up to 100,000 attendees can be planned through the Microsoft 365 assistance program.
External Guests	Externals that have been invited can click to join or present	Anyone that's been invited can click to join (or present if access has been granted)	An MoE guest account is required for an external guests to attend or present
Interaction	• Participants up to 1,000 have fully interactive equal meeting capabilities. • Participants over 1,000 up to 20,000 have View-only capabilities.	• Participants up to 1,000 have fully interactive capabilities. • Participants over 1,000 up to 20,000 have View-only capabilities. • Audience interaction configurable. • Can specify presenters.	• Broadcast to large audiences. • Moderated Q&A for audience interaction. • Can specify producers and presenters, including external presenters. • Supports more advanced production capabilities.
Number of Presenters	Any attendee can present at any stage of the meeting. However only one can at any given time.	Up to 1000 - Any presenter can present at any stage of the meeting, one at a time.	Up to 10
Time Limit	None	None	4 Hours (currently 16 hours per broadcast until end of 2021 due to COVID)

			NB: 50 events can be hosted simultaneously across an M365 tenant
Registration	No	Yes	No
Ability to disable cameras	No	Disable all attendee cameras, with the ability to enable/disable individually	N/A – view only
Ability to disable microphones	Mute only, participants can turn back on when desired	Yes, with ability to enable/disable individually	N/A – view only
Chat	Yes (Presenters and Attendees all see the same Chat)	Yes (Presenters and Attendees all see the same Chat)	Only for Producers/Presenters to use/see
Q&A	No	No	Yes
Polls	Yes - Forms-powered polls in meetings also support guests	Yes - Forms-powered polls in meetings also support guests	No
Reactions (Emojis)	Yes (Can be turned off)	Yes (Can be turned off)	No
Lobby	Yes (Can be turned off)	Yes (Can be turned off)	No
Break Out rooms	Yes	Yes	No
Live captions and subtitles	Yes	Yes	Yes
Filter			

Document 2

Information and Communication (IT) use Policy

Introduction

This policy provides important information for all users of Ministry provided ICT tools and systems (including laptops, mobile devices, software and networks) to ensure you maintain the confidentiality, availability, integrity, and legal compliance of information held electronically by the ministry.

Your obligations

Every person provided with a Ministry user account (including employees, contractors and consultants) and/or Ministry ICT tools and systems is responsible for ensuring the Information Security (InfoSec) of any information you have access to, and that you always remain compliant with permitted uses.

You are specifically required to consider the classification of the data you have access to and to ensure usage both internally and externally is appropriate to that classification. I.e. *"Is this appropriate to be circulated externally"*

You will also be required to set and maintain a unique password which is to be kept strictly confidential and to enroll in a biometric system that protects your Ministry user account from unauthorised use via the use of two factor authentication methods.

What is permitted and what is not

Permitted

All access to Ministry systems you have been granted access to, that are a requirement of your role. Should you change roles these permitted uses may also change.

Limited reasonable personal use of ICT tools and systems. This includes:

- Online banking
- Reading the news
- Checking email
- Phone calls
- Text messaging

Not Permitted

Staff must never use the ICT tools or systems for non-permitted activities. This includes (but is not limited to):

- Any activity, behavior or action that may put children at risk.
- Endangering or causing distress to any other person through harassment, bullying or intimidation.
- Defaming any person or organisation.
- Any action or inaction in relation to ICT systems that could bring the ministry into disrepute eg, statements of a political nature.
- Soliciting, disclosing or trading for personal gain or profit.
- Gambling of any nature.

- Generating, accessing, saving, storing or sending pornographic, sexually explicit or offensive material, remarks or proposals.
- Downloading, distributing or storing unnecessarily large software, multimedia files or any other material that could disrupt ministry ICT systems
- Sending and/or participating in mass mailing.
- Visiting sites that allow the downloading of unauthorised non-certified software or their contents including hacking, cracking, malicious software or scripting.
- Frequent, extensive or illegal personal use of email, internet or phone.
- Registering ministry addresses on internet sites as an address for any inappropriate material to be forwarded by email.
- Downloading commercial software in violation of its copyright or licensing agreement or downloading unauthorised or illegal software.
- Any internet use that interferes with the production of business unit outputs or costs the ministry an unacceptable amount of money (such as using your Ministry provided phone as a hotspot for others)
- Knowingly causing interference with or disruption to any network, information service, equipment or any use by deliberate propagation of virus, trojan horse, trap-door, back-door or any other malicious programme code.
- Using any system or software with the express intent to circumvent Ministry controls (including forwarding or uploading ministry data to personal email, file shares or other such systems)
- It is important to use only approved Ministry software and applications on your Ministry supplied devices. Click here to find more information.

If you're ever in doubt about what is permitted, check with the service desk or speak to your people leader.

Qualifying for a Ministry supplied Mobile Phone

Managers are responsible for ensuring Ministry mobile phones are only allocated if staff members meet the following criteria;

- Staff member is either **permanent or fixed term staff** and
- provides 24 / 7 support; or
- is required to work away from a MoE office or home on a regular basis; or
- works regularly in a remote location; or is
- required for Health and Safety compliance.

Policy Breach and Reporting

Any privacy breach or any security breach **must be reported immediately** to the ministry's Health, Safety, Security and Privacy team, **without exception or delay.**

People leaders and staff are expected to understand and apply the Privacy Principles of the Office of the Privacy Commissioner.

In the event of a breach of the ICT Use Policy, appropriate action will be taken. The nature of this action will be considered on a case-by-case basis. **Dismissal may result** following a serious breach of the policy. The Ministry may also review the contractual relationship of any contractor (paid by invoice) who breaches this policy.

Breaches of the policy may, depending on the circumstances, constitute an offence under the Crimes Act, Copyright Act 1994, Videos and Publications Classification Act 1993 or other legislation. Such breaches may be reported to the Police or relevant enforcement agency. Individuals may also face liability for loss or damages under the following Acts:

- Privacy Act

- Defamation Act
- Human Rights Act
- Other relevant legislation

Getting help with this policy

For Everyone

- Education Service Desk
- (04) 463 8446 ext 48446
- If you need any help or have any questions, please contact the Education Service Desk.

Filter

Document 3

Organisation Information privacy & security policy

Information privacy and security policy

Overview

Ministry data and information, irrespective of the form in which it exists, must be protected from unauthorised access, modification or accidental loss. Systems, whether computerised or manual, must also be able to provide accurate and reliable information to authorised recipients at the time it is needed.The information privacy and security policy is intended to ensure that:

- Ministry information, irrespective of the form in which it is exists, is protected from unauthorised access, modification, disclosure or loss of Ministry systems, whether computerised or manual, are protected from internal and external threats, while still being able to provide the required accurate and reliable information to authorised recipients at the time it is needed
- the transmission, storage and disposal of data/information complies with statutory requirements and Government directives.

The approaches described here apply to all Ministry staff/functions and are intended to complement centralised IT approaches e.g. for cybersecurity.

Purpose

The purpose of this policy is to protect the information for which Te Tāhuhu o te Mātauranga | Ministry of Education (Ministry) is responsible for against loss, theft, unauthorised modification or in appropriate disclosure.

Organisational scope

This policy applies to all Ministry staff and contractors who have access to Ministry information and information systems as well as the owners of the Ministry's information and related systems.

Definitions

Refer to data / information within Te Tāhuhu: classification for security / privacy.

Policy principles

The following principles guide the Ministry's approach to security and inform security policies and controls.

- Duty of care: responsibility for information security on a day-to-day basis is every user's duty. Specific security responsibilities may be allocated according to an individual's role within the Ministry, however all employees, including contractors and consultants, will be required to complete Multi Factor Authentication (MFA) on the first day of employment at the Ministry.
- Privacy: information can only be collected and used for the purpose it was intended. It is unacceptable for users to make unauthorised use or disclosure of personal information to which they have had access in the course of their employment.
- Confidentiality: ensuring only the people who are authorised to have access to information are able to do so and that information is released in a proper manner.
- Integrity: information is protected from unauthorised modification to protect its value.

- Availability: ensuring information is available when required to support critical business processes.
- Integrated: business systems will be developed with security in mind and will employ common security services and standards wherever possible.
- Risk based: security controls are appropriate for the level of risk.
- Sector alignment: security policies and controls should align with Government and Education Sector initiatives.
- Audit: business processes, and the systems that support them, will be subject to regular audit to ensure appropriate information use.

In order to achieve these principles:

- the Ministry computer networks should only be accessed and used for supporting business needs
- private use or unauthorised disclosure of Ministry information is strictly prohibited
- all users are responsible for taking care in their actions and work practices to ensure information is kept secure at all times
- the Ministry has the right to actively monitor and audit the usage of its computer networks to protect its interests. This extends to making information held on the Ministry's networks available to managers, the police or other appropriate authorities at the Ministry's discretion.

Access to and release of information: accountabilities

Users

Users are responsible for:

- •completing Multi Factor Authentication (MFA) on the first day of employment at the Ministry
- ensuring that information in their care is kept secure at all times
- ensuring that sensitive information is transmitted securely only to the intended recipient
- taking due care with information stored on mobile devices
- not sharing identity information such as passwords etc.

Owners

Owners of IT systems, or sets of information held electronically are responsible for:

- identifying those who are to be provided access to information assets and the rights that they are granted
- delegating authority to those that may grant access rights to others on behalf of the Custodian
- ensuring that their systems or information sets have security controls in place corresponding with the assessed risks associated with the information assets contained therein.

Managers

Managers are responsible for:

- ensuring all users are aware of and comply with this policy and associated guidelines including completion of Multi Factor Authentication on the first day of employment at the Ministry.
- arranging for security education and training where appropriate.
  NB: Managers may wish to provide new employees with the Multi Factor Authentication (MFA) Guide and the Multi Factor Authentication (MFA) Question and Answers file.
- Complete Multi Factor Authentication (MFA) during the first access to Ministry documents on the first day of employment at the Ministry.

IT Group

IT Group is responsible for:

- operating a service desk function for identity management (password changes, account creation etc)
- providing a secure IT environment
- formulating and promulgating an operational IT security policy
- developing and maintaining of a security architecture
- providing security related advice to IT projects.

Reporting of privacy or security breaches

Any privacy breach or any security breach must be reported immediately to the Ministry's Health, Safety, Security and Privacy team. All other security breaches must be reported to the Ministry's Security Officer (Zoe Griffiths, Haūtu - Rangatōpū | Deputy Secretary - Corporate).

Data / information types and classification

The rollout of Electronic Document and Records Management (FileNet) in the Ministry facilitates the sharing of documents and records internally throughout the organisation. For our information systems to facilitate sharing of and collaboration on documents across the Ministry information must be open to all authenticated staff members by default and only secured by exception. This policy establishes the principle of information transparency in the ministry while also outlining our obligation to secure certain kinds of information internally (as well as externally). All Ministry staff and contractors acting on behalf of the Ministry are responsible for storing information in a manner which facilitates appropriate access. By default, this means that information is accessible throughout the Ministry, information is therefore only restricted by exception.Ministry staff are expected to:

- manage information as a Ministry (rather than a personal or team) asset
- store information in a manner so that it is accessible as widely as appropriate according to its classification
- exercise good and consistent judgement in the application of security to information.

Documents that relate to or concern the following must be secured:

- personal or public safety (eg School Security)
- national security and international relations (e.g. briefings on visiting dignitaries)
- sensitive personal information (eg Personnel files, Special education Case files, databases containing student level data including names)
- embargoed material (eg pre-released budget documents)
- any other material for which internal release would pose an unacceptable risk to the Ministry.

Managers are responsible for determining what material fit these descriptions, but in general terms, information should be secured if:

- release would expose the Ministry to litigation
- information is likely to be misconstrued in a manner which will cause embarrassment to the Ministry
- release would violate contractual obligations
- information is embargoed (eg media releases).

Managers and staff are expected to understand and apply the Privacy Principles of the Office of the Privacy Commissioner. Managers and staff are expected to pro-actively consider, for particular material (documents, spreadsheets, databases, etc):

- how it should be secured internally
- processes that should be applied in any transmission of material outside the Ministry.

This policy should be read in conjunction with:

Getting help with this policy

For all staff

- Security Team
- security.team@education.govt.nz

9(2)(a)

Filter