Videoconferencing Guidelines

[Out of Scope]

Published 11/09/2023

There is only one video conferencing technology approved for use at ACC. That is Microsoft Teams, used on desktop computers and Surface Pros.
Please visit https://accnz.sharepoint.com/sites/M365Hub/SitePages/Microsoft-Teams.aspx for Microsoft Teams instructions.

Alternative videoconferencing software (e.g., Zoom, Blue Jeans, Google Hangouts etc.)
The rules for videoconferencing software do not differ from any other software at ACC. Ask yourself: is this software part of ACC's enterprise portfolio of software or services? If the answer is no, then don't use it. If you do not know the answer, then don't use it. Shadow IT is not safe for use at ACC as it hasn't gone through:

- Consultation with Architecture.
- A privacy and ethics assessment with Privacy.
- Certification and Accreditation (C&A) with Information Security.
- The procurement process with ICT Contracts and Commercial.

For any software to be used enterprise-wide, there would need to be a business case presented to executive (tier 2 management) establishing the business need for the software, and to show why existing enterprise software is not fit-for-purpose. Then, provided the business case is approved, a project team would need to be established and funded to bring about the change.

Nevertheless, there are external organisations (including government agencies) that have adopted different videoconferencing software from ACC as part of their enterprise system. They may not be able to use Microsoft Teams to host their meetings, and you may need to accept invites to their meetings as part of your job. If this is the case, you may accept an invite to the meeting, but just remember:

- Do not host any meetings.
- Use the web application version rather than the desktop application (as this requires an install).
- Make sure you only accept meeting IDs with PINs, not open meeting links.
- Make sure you know who is in the meeting, so that you can adjust your dialogue accordingly.
- Join without video initiated until you are comfortable the audience is as expected.

Records
Decisions or actions made during videoconferences you participate in are likely to be official records. ACC is legally obliged under the Official Information Act, Public Records Act and other legislation to make and keep a record of all the decisions or actions made during videoconferences that form part of ACC's normal work practices. A transcript or video recording of the meeting meets these obligations, as do formal meeting notes. If in doubt, please email IDT@acc.co.nz.

Frequently Asked Questions

What if we really need to host videoconferences in Zoom/Blue Jeans/Google Hangouts/other?
You can use Microsoft Teams and invite external participants. They can join from an internet browser, or they may choose to install the desktop client and join anonymously with the free version of Teams. If your business group leadership believes that an exception needs to be made, and the use of alternative videoconferencing software be approved, they may escalate the issue. More information about inviting external participants to Microsoft Teams is here.

What if I have already downloaded Zoom/Blue Jeans/Google Hangouts/other?
You will need to uninstall the application and change any passwords used in these applications. (Note: It is preferred that you DONT use your ACC email address as the user ID for these systems).

Can I turn my video on when invited to a Zoom/Blue Jeans/Google Hangouts/other meeting?
Use your discretion. If the meeting replaces what would normally be a phone call, there is no need to turn your video on. If the meeting replaces what would normally be a face-to-face meeting, then you may want to enable video. Just make sure you check what's in your background before enabling other meeting participants to see you.

I prefer alternate technologies to host video conferences, like Zoom/Blue Jeans/Google Hangouts/other. Why can't I use those?
These have not been endorsed for use across ACC. The enterprise solution is Microsoft Teams. If your leadership team believe this is not fit for purpose to meet your capability requirements, then they may want to escalate the issue.

Meeting technology

Online Meeting Technology

See our Videoconferencing Guidelines regarding use of other apps like Zoom/Google Hangouts/Blue Jeans etc

Microsoft Teams

Our primary tool for online meetings is Microsoft Teams - it can be used on your laptop or enrolled mobile phone to have an online meeting with a group of people (including people who are external to ACC), or a one-one video call. You can record meetings and share the recording afterwards.

For information and user guides see Microsoft Teams Meetings.

Skype for Business

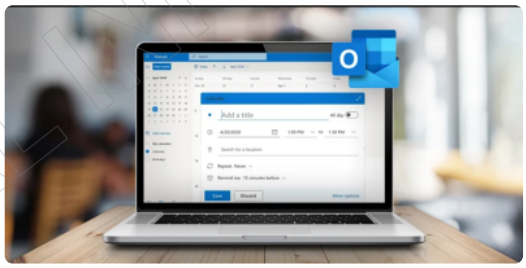
Microsoft are discontinuing this application - Please use Microsoft Teams for online meetings.

WebEx

WebEx is a tool used at ACC by some groups for online training, job interviews or meetings. It is recommended that you consider using Microsoft Teams for meetings where possible.

For information on setting up and using WebEx see this page.

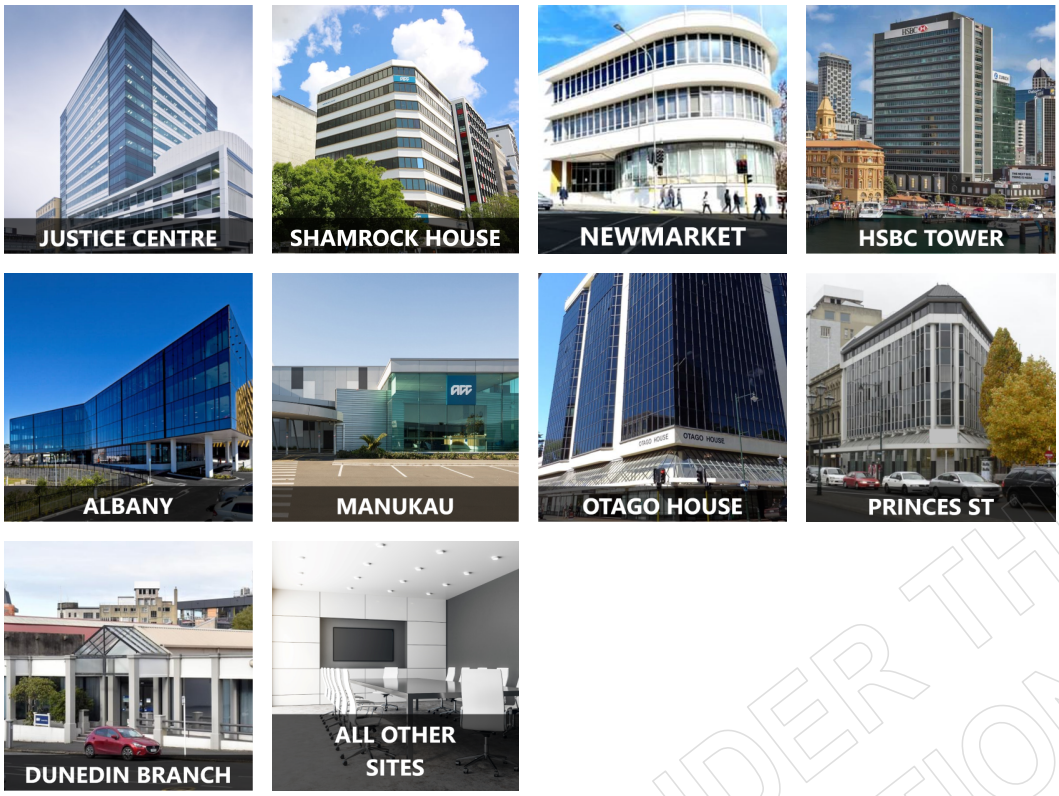
Meeting Room Technology



Booking meeting rooms

You can book meeting rooms via Outlook using these instructions.

Which site's meeting room technology do you want to find out about?



Audio Conferences

We no longer use audio conferencing at ACC. If you wish to have an audio meeting with others, you can do this via a Microsoft Teams meeting.

To order polycom meeting room phones:

1. Open ICT Self Service
2. Click on 'Telephony'
3. 'Other telephony items'
4. 'Meeting Room phones'
5. Request access and complete the form

Which M365 communications channel should I use?

GOV-027692 Appendix

CommunicationChannels

Title	Outlook	Teams	Viva Engage	SharePoint	Te Pātaka	Skype	Stream
External Messages	✓	—	—	—	—	—	—
Formal Messages	✓	—	—	—	—	—	—
Targeted messages	✓	—	—	—	—	—	—
Updating other teams	✓	—	—	—	—	—	—
Planning and discussing	—	✓	—	—	—	—	—
Asking your team questions or polls	—	✓	—	—	—	—	—
Prompt group problem solving	—	✓	—	—	—	—	—
Chat	—	✓	—	—	—	✓	—
Online meetings	—	✓	—	—	—	✓	—
Large scale presentations (250+)	—	✓	—	—	—	—	—
Sharing useful insights	—	✓	✓	—	—	—	—
Social posts	—	✓	✓	—	—	—	—
Asking questions or running polls outside your team	—	—	✓	—	—	—	—
Sharing news or information to interested communities	—	—	✓	✓	✓	—	—
Sharing news or information to All ACC	—	—	✓	✓	✓	—	—
External phone calls	—	—	—	—	—	✓	—
Storing & sharing videos	—	—	—	✓	—	—	✓

A deeper look at our channels

(Their uses and attributes)

Outlook

Use for:

- Formal messages
- Targeted messages to people outside of your team
- Messages to people outside of ACC
- Messages which do not require an immediate response

Attributes/Features:

Microsoft Teams

Use for:

- Planning, discussing, asking your team questions
- Sharing files with your team
- Accessing shared team resources
- Prompt problem solving discussions
- Private chats with individuals and groups
- Online meetings*

- Formal
- Useful for targeted messages to people outside of your team
- Ability to message people outside of ACC
- Accessible to enrolled mobiles

More information

- Visit the Outlook page.

SharePoint (Communications Site)

Use for:

- Sharing information with others at ACC via a site you can manage yourself
- Large scale presentations to audiences over 250 people (Live events)
- Sharing insights that are useful for others
- Social posts

Attributes/Features:

- Informal
- Transparent
- Connected to a pre-set business unit or community
- Private chat (chat history remains view-able in chat)
- Video conferencing, with recording, for meetings of less than 250 people
- Video presentations (Live events), with recording, for up to 10,000 participants
- Provides a window to other Microsoft 365 apps and is intrinsically linked to SharePoint
- Accessible to enrolled mobiles

More information

- Visit the Microsoft Teams page.

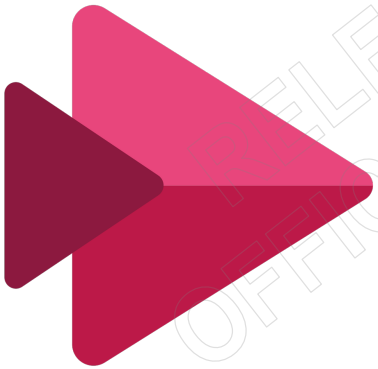
- Discussing/making suggestions while co-authoring documents

Attributes/Features:

- Blog styled stories for a predefined audience
- Co-authoring communications through comments

More information

- Visit the Digital Workspace page.
- Visit the SharePoint page.



Stream

Use for:

Skype for Business

Use for:

- External phone calls

Attributes/Features:

- External calling
- Chat functionality (chat history accessible in Outlook)
- Video conferencing, no recording (250 participant limit)

More information

- Visit the Skype for Business page.

- Storing and sharing work-related videos internally at ACC

Attributes/Features

- ACC's internal video platform
- Auto transcription
- Auto-timeline of who spoke in Meeting recordings
- Video can be sorted by Group or Channel
- Videos can be embedded into SharePoint sites

More information

- Visit the Stream page.

Viva Engage

Use for:

- Leveraging the expertise of people outside your circle
- Sharing your team's updates with a wider audience
- Sharing insights that are useful for others
- Recognising/celebrating exceptional performance with a wider audience
- Social posts

Attributes/Features:

- A discussion forum accessible to all ACC staff
- Wide membership base
- Open and transparent

- Ability to create interest groups
- Yammer feeds embeddable into SharePoint sites
- Customisable feeds

More information:

- Visit the Viva Engage page

For more information on all of the M365 apps and what they do, click here.

Using unsanctioned apps/sites/tools? Touch, Pause, Engage

[Out of Scope]
Technology Enablement Manager 00514472

Are you using a free app or trial subscription for work purposes? Are you communicating online with your team using something other than Teams, Outlook or Skype?

Using apps, websites and technology that haven't been through ACC's approval process opens us up to all kinds of risks. Online/mobile websites and tools can store your data insecurely and share or sell it to others without your knowledge. When this involves communication with your ACC colleagues or any information relating to your ACC work, it can also create privacy breaches and break our obligations under the Records Management Act as we don't necessarily have control over where that information is stored, how long it is retained for, or how it can be accessed.

If you have a requirement please check out tools we already have available (see below for a list of our main Microsoft/Atlassian apps) then, if you still feel like they don't meet your needs, contact the Architecture Team and they'll look at what other options might be available and will explain the process you'll need to follow if you want to get approval to use something different. It's really important you don't just start using something just because it's free or because you think it looks useful.

Here's a little rugby scrum term for you to put into play....

- **Touch** base with your team to check what they're using and why
- **Pause** any use of tools outside our sanctioned list
- **Engage** with the Architecture Team to discuss any special requirements and what you need to do regarding information that may already be in unsanctioned tools

WebEx

WebEx is a tool used at ACC for online training, job interviews or meetings. It is recommended that you consider using Microsoft Teams which incurs no cost. WebEx provides some features that Microsoft Teams doesn't such as 'break-out' online meeting rooms which can be useful for large training sessions.

Only hosts of a meeting need to set up a WebEx account. Attendees of meetings or training sessions do not have to sign up.

Meeting attendees will get a meeting invitation by email; all they need to do is follow the instructions given.

Set up a WebEx account

If you don't have an account but need to set up a meeting:

1. Visit ICT Self Service
2. Click on the Applications icon
3. Click on WebEx towards the bottom of the page
4. Complete the drop-down lists
5. Click on Add

Your order will then be processed, and you'll be given access. You will receive a host account user name and initial password.

Save the ACC WebEx URL: https://accnz.webex.com as an Internet favourite for future use.

Costs

Costs for using WebEx are always charged back to the Host's cost centre, for all participants.

Charges for WebEx are 35 cents (NZD) per minute/per person in attendance.

WebEx tips and etiquette

Some useful tips and etiquette to ensure your WebEx sessions are enjoyed by all participants:

- Let colleagues near you know you're taking part in a WebEx meeting, by putting up a sign or sending them an email.
- Ensure your phone is off divert before joining a session, otherwise you may have difficulty with the teleconference 'call-back'.
- If you are an attendee at a meeting, close all other applications on your desktop, especially your email.
- Use the 'raise hand' function in WebEx to ask the host/facilitator a question, instead of interrupting.
- Mute your phone (using the mute button in WebEx) when not talking. An X appears next to your name, letting other attendees know you are on mute.

Telephony Policy

POLICY NUMBER	5.11.0 (Level 3 policy)
TOPIC	Telephony - Subordinate to Information Security policy
OWNER	[Out of Scope] Manager, Digital Workspace and Engineering Technology and Platforms Enterprise Change Delivery Group
DATE APPROVED	2 February 2021
APPROVER	[Out of Scope] Head of Technology and Platforms in consultation with [Out of Scope] Deputy Chief Executive – Enterprise Change Delivery (DCE-ECD)
DATE OF REVIEW	2 February 2023

1 Objective

We use telephony services to communicate internally and externally. Telephony devices are increasingly used to collaborate and share information within ACC. Telephony services must be appropriately used by and available to ACC employees, whilst adhering to good information management practice and relevant legislative requirements.

2 Scope

This Policy applies to all ACC employees, contractors and persons using ACC telephony devices, or personal Telephony devices (known as Bring Your Own Device or BYOD) used for ACC business.

Specific telephony and meeting guidance available via the Technology Hub – IT Support Resources and M365 Hub will cover in detail the use of the following equipment and services:

- Mobile phones and other mobile devices, where not explicitly covered in Policy Principles listed below
- Bring Your Own Device (BYOD) including mobile phones and tablets
- Skype for Business
- Microsoft Teams
- Genesys (Contact Centre)
- Other telephony or Voice over Internet Protocol (VOIP) services:
  - Audio and video conferencing
  - Webex (Online meeting rooms)

Call recording where used will be captured in the platform specific standards for each device or application. All call recording using telephony solutions will be compliant with the ACC Privacy Policy and any applicable legislation.

3 Policy statements

3.1 **We use ACC provided telephony services and devices primarily for business purposes.**

We may use ACC provided telephony services and devices for personal use, without reimbursing ACC, provided their use is in accordance with the following:

- Personal use is not excessive and is in accordance with the Mobile Device Reasonable Usage guidelines.
- All personal use must be compliant with the ACC Use of the Internet Policy and Information Security Policy and associated standards.
- Personal calls using ACC telephony devices should only be made within New Zealand unless prior management approval has been given.
- Personal use must always be in accordance with the ACC Code of Conduct.

3.2 **We secure and manage telephony devices to enable employees to securely communicate, collaborate and access information internally and externally.**

- We will encrypt all ACC data on devices using Modern Device Management (MDM).
- Where appropriate, MDM may restrict, or control, device functions and/or applications to secure ACC data.
- The MDM solution will allow both corporate and personal applications on the same device.
- Single Sign On (SSO) with Multi Factor Authentication (MFA) will be supported for all ACC telephony applications.
- If a device is lost/stolen, we will use the MDM solution to access GPS location data and remotely wipe a device, and/or applications and data.

3.3 We dispose of telephony devices according to government requirements.

- All telephony devices purchased by ACC remain the property of ACC and cannot be sold or gifted to any other party without the approval of the Deputy Chief Executive – Corporate & Finance.
- Equipment that is no longer needed or is to be disposed of must be returned to the Enterprise Change Delivery group for removal of ACC data and subsequent disposal in accordance with the New Zealand Information Security Manual (NZISM) requirements.

3.4 We do not use unapproved telephony devices within ACC.

- Use of unapproved devices is a breach of ACC's Code of Conduct and may result in disciplinary action.
- All mobile telephony devices, including BYOD, must be enrolled in, ACC's MDM platform when being used for ACC business purposes.

3.5 We ensure all call recordings made are in accordance with best practice and legislation.

- ACC does not allow call recording without the informed consent of all parties involved.
- Where a call recording forms part of the decision-making process, a copy, or verified transcript of the call must be saved in the appropriate system of record.
- Where covert recording is required for an investigation, approvals must be obtained and retained in line with the Integrity Information Gathering Policy.
- Where a call recording is to be published e.g., record of a meeting, informed consent must be sought from all persons involved.

3.6 We ensure all telephony devices used in ACC are fit for purpose.

- All telephony devices used for ACC purposes must be updated to, at a minimum, the most current version of the operating software for that device -1 iteration (n-1)
- All ACC provided mobile devices must be managed using the ACC MDM solution to ensure all relevant updates are delivered and installed correctly.
- Mobile telephony devices that are compromised or no longer fit for purpose may have all ACC data and applications remotely wiped from that device using the ACC MDM solution.

3.7 We control the access to our data and systems that we allow telephony devices to have.

- ACC applications are deployed, controlled and encrypted by our MDM solution on mobile devices.
- Any mobile application that has access to ACC credentials or data must be managed by the MDM solution.
- All ACC applications deployed on mobile devices will be monitored and any suspect activity investigated accordingly.
- Where required ACC may enforce device encryption and/or strict device management where it is deemed necessary according to the ACC Modern Device Standards and Guidelines.

3.8 We protect ACC data on mobile devices.

- All mobile applications that hold ACC data or credentials, or access ACC's internal network, must comply with the certification and accreditation requirements set out in the Cloud Computing Policy.

3.9 We apply ACC Privacy and Information Management Policies across all our telephony platforms.

- Where a system stores personal information, using telephony devices, it must be done in accordance with ACC Privacy and Information Management Policies, Standards and Procedures.
- We must ensure that information gathered via telephony devices is transferred to the appropriate system of record (e.g., Eos) as appropriate.

4 Accountabilities

The Manager Digital Workspace and Engineering with assistance from the Chief Information Security Officer (CISO) is responsible for this policy being implemented on behalf of the Deputy Chief Executive – Enterprise Change Delivery (DCE-ECD).The DCE-ECD retains overall accountability for this policy.

This level three Policy will be reviewed every two years, or when significant changes occur.

5 Responsibilities

We are collectively responsible for the safe and proper use of telephony devices at ACC.

Roles:	Responsibilities:
Employees including contractors, consultants and temporary employees engaged by ACC	• Comply with this policy and any supporting standards • Complete, and comply with, all required training modules • Observe proper telephony etiquette • Report any lost/stolen ACC owned mobile devices to the IT Service Desk as soon as possible and inform their manager.

People managers	• Must demonstrate good telephony behaviours. • Must address telephony issues with the appropriate employees. • People Managers are responsible for ensuring their employees and contractors are aware of the ACC Telephony Policy. This means: • Identifying employees, including contractors and fixed-term employees, that require training and taking appropriate action to address this. • Modelling good practice in telephony management to their employees
Digital Workspace team and Information Security team	• Assist to maintain and administer this policy and associated standards • Monitors, via the ACC MDM and internet security tools, compliance with this policy • Liaise with telephony suppliers to detect and prevent security risks and misuse of telephony devices • Detect, Investigate, and troubleshoot telephony security issues and threats • Report on and plan for security incidents and threats • Work with the ACC telephony provider to manage day to day asset management of ACC owned/provided devices. • Record breaches of the policy and escalate where appropriate (DCE-ECD, People Managers or Talent).

6 Monitoring and oversight

The Digital Workspace team with assistance from the Information Security team will monitor compliance with this policy. Day to day oversight of employee's compliance is the role of line managers.

The personal use of telephony services is monitored and is at the discretion of ACC. Where unfair or inappropriate use is found, disciplinary action may be taken. This may include cessation of service, and/or that the employee reimburses ACC.

The monitoring and oversight of Telephony follows the five lines of assurance model.

LOA	Role	Monitoring & Oversight
1st Line	Employees and People Managers	• All employees remain alert to potential breaches of the Policy and report potential and actual breaches to their manager. • All people managers ensure that (i) breaches brought to their attention are documented**1**, (ii) notification of the breach is provided to the owner of the Policy within five days of the breach occurring. • From time to time we deliberately take actions contrary to a policy's provisions (corporate policy exceptions). When people managers are responsible for a corporate policy exception, the people managers ensure that the exceptions are agreed either using the process in the Policy or by agreement in writing from the Policy owner.
	Group Risk and Compliance Manager and/or Advisor (If applicable)	• Supports employees to determine whether events constitute actual breaches of the Policy. • Escalates breaches to the Group's Leadership Team and Deputy Chief Executive when appropriate • Updates risk registers as required.
	Policy Owner	• The Policy Owner ensures that the Group (and other parts of ACC if applicable) respond appropriately to Policy breaches and requests for exceptions.
2nd Line	Enterprise Risk Team	• Performs periodic oversight activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of the Group's practices to monitor compliance and deal with breaches. • Reports to the Executive and the Board on the outcomes of such activities.
	Digital Workspace team & Information Security team	• Performs monitoring, via the ACC MDM and internet security tools, compliance with this policy • Report on and plan for security incidents and threats • Record breaches of the policy and escalate where appropriate (DCE-ECD, People Manager or Talent)
	Talent	• Supports the management breaches in relation to Code of Conduct or Discipline Policy
3rd Line	Internal Audit (and external providers)	• Performs periodic audit activities intended to assess and/or provide insights into (among other things) compliance with the Policy and the adequacy and effectiveness of the Group's practices to monitor compliance and deal with breaches. • Reports to the Executive and the Board on the outcomes of such activities.

[1] The "Policy Breach Template" can be used for this purpose but is not mandatory.

LOA	Role	Monitoring & Oversight
4th Line	Executive	• Ensures each Group has sufficient emphasis on risk management and meeting compliance obligations. • Ensures effective processes and monitoring are in place to meet compliance obligations for the Policy. • Acts in an appropriate and timely manner in response to reports received that alert the Executive to opportunities to improve Policy compliance activities.
5th Line	Board	• Responsible for approving any material changes to the level 1 Policies, including text related to monitoring and oversight of compliance with the Policy. • Acts in an appropriate and timely manner in response to reports received that alert the Board to opportunities to improve Policy compliance activities.

7 Breaches of Policy

Compliance with all policies and procedures is required under ACC's Code of Conduct. Behaviour or actions that are investigated and found to be in breach of the Code of Conduct may result in disciplinary action. Refer to Code of Conduct for further information.

Deliberate non-compliance or circumventing of the requirements of this policy is deemed to be serious misconduct.

8 Contacts

Report any lost/stolen ACC owned mobile devices to the IT Service Desk as soon as possible. For general policy queries, contact Digital Workspace team or Information Security, infosec@acc.co.nz.

9 Definitions

Telephony	Telephony is the field of technology involving the development, application, and deployment of telecommunication services for the purpose of electronic transmission of voice, fax, or data, between distant parties. "Telephony" has been used as a proxy for all voice communications.
Bring Your Own Device or BYOD	The use of personally owned telephony devices for ACC business purposes.
Modern Device Management (MDM)	Modern Device Management is a set of tools and processes that allow us to work flexibly on various corporate and personal devices. For the purposes of this policy MDM also includes Mobile Application Management (MAM) and associated technologies.
Mobile device	A portable telephony device that can be used for voice communications outside of an ACC office or network. For the purposes of the ACC MDM solution – any telephonic device that has a SIM card and can independently connect to the internet or a mobile network is considered a mobile device.

10 References

Information Management Policy
Information Management Standards
Information Security Policy
Information Security Standards
Code of Conduct
Privacy Policy
Cloud Computing Policy
Copyright Policy
Use of the Internet Policy
BYOD Policy
ACC Modern Device Standards
Mobile Device Reasonable Usage Guidelines

11 Version Control

Version	Date	Change reason	Who
0.1	08/01/19	Draft added to template	[Out of Scope]
0.2	10/01/19	2nd draft after feedback from focus group	
0.3	25/03/19	Update with feedback	
0.4	26/06/20	Reviewed and updated document – resolved outstanding comments	
0.5	27/08/20	Updated template and standardised the 5 LOA	
1.0	02/02/21	Updated group name to Technology & Innovation Final	
1.1	26/10/22	Updated roles to reflect organisational structure changes	