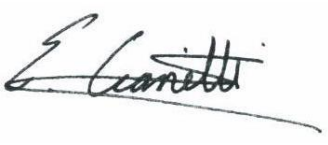
APPLIES TO STRATEGIC POLICIES ONLY

This an official copy of the **Electronic Recording and BYOD Usage Policy**, made in accordance with the provisions of *Local Government Act and Regulations, Public Records Act, Mount Isa City Council's Local Laws, Subordinate Local Laws and current Council Policies.*

Strategic policies are adopted by Council due to its desire to influence the direction of an issue or assist in the delegated decision making of Council officers. Strategic policies should follow the jurisdiction provided to Council through its Corporate Plan; the **Electronic Recording and BYOD Usage Policy** is approved by the Mount Isa City Council for the operations and procedures of Council.



.....
Emilio Cianetti
Chief Executive Officer

DOCUMENT VERSION CONTROL					
I/R	982920	**FILE**	1208 Policy Register	**POLICY TYPE**	Strategic (Council)
VERSION	**DATE**	**RESOLUTION NO.**	**DETAILS**		
V1	09/11/2014	OM09/11/14 Adopted	**Responsible Officer** Senior Human Resources Officer **Description** Document Creation – New Document		
V2	24.11.2015	OM08/12/15 Amended	**Responsible Officer** Senior Human Resources Officer **Description** Formatting Only		
				REVIEW DUE	11/2017 *Review by Council*
				EXTINGUISHED	00.00.0000 Resolution No: OM00/00/00 *No further action required.*

POLICY STATEMENT

This policy provides Council employees, contractors and volunteers with direction that enables greater transparency, accountability and efficiency in relation to the management of 'photography or recording' and appropriate use of Bring Your Own Devices ("BYOD").

MICC must take reasonable steps to protect its' visitors, employees and contractors from unauthorised photography or recording and from inappropriate use of BYOD.

The guidelines below apply to all photography, imaging, audio, video, or other electronic recording of visitors, employees, others persons within a MICC facility and or where MICC is operating or conducting business (i.e. jobsites and general public areas) whether from a MICC allocated device or a 'Bring Your Own Device' (BOYD).

The guidelines in relation to BYOD usage apply to all usage of BYOD by Council employees.

This Policy is subject to the *Local Government Act 2009* and the following five (5) principles.

Positive: The reason for recording others must be for a positive purpose and not in an attempt to trap, bully or intimidate;
Permission: Must always be obtained prior to the recording of employees, contractors and members of the public;
Privacy: Must be respected at all times;
Protect: Work related data and access to that data must be protected from unauthorised access;
Preserve: Work related data (including data that is held on a BYOD) must be preserved by saving it to MICC's Document Management System.

COMMENCEMENT AND APPLICATION

This policy will commence from the date of Council resolution and replaces all other existing Electronic Recording or BYOD usage policies (whether written or not). This Policy applies to all MICC employees regardless of their employment status, role or position and to all MICC contractors and volunteers, except as stated otherwise within this Policy.

This policy regulates contracts of employment and contracts for services and applies alongside but not part of any employee's contract of employment and other contracts of (for) service with agents, external labour personnel (including temporary Contractors) and volunteers of MICC.

POLICY INSTRUCTION

1. RESPONSIBILITIES IN RELATION TO ELECTRONIC RECORDING AND PHOTOGRAPHY

1.1 The following must be observed by all persons subject to this Policy:-

a) A person may record and photograph other people (including members of the public);

b) The person creating the recording or photograph must be part of that conversation, interaction or event;

c) The person creating the recording or photograph must advise the other party/parties that they will be recorded. Should a person being recorded or photographed object to being recorded or photographed, the person must cease recording and refer the matter should be referred to the person's Manager for resolution. A person cannot continue to record or photograph whilst in transit or walking around the office/an area. Otherwise, conversations/interactions and images may be recorded that the person recording or taking the photograph is not a party to and it is possible that the person being recorded will not understand that they have been recorded or photographed;

d) All parties involved in the conversation, interaction or event must be provided a copy of the recording or photograph or be directed to Councils' Document Management System stating where it can be located;

e) A person must not provide a copy of the recording or photograph to any member of the public or a third party entity (including another Council contractor) unless required to by law;

f) In response to a formal application from a member of the public or a third party entity for access to a recording or photograph under the *Right to Information Act 2009* or *Information Privacy Act 2009*, the application will be processed by a responsible officer in accordance with MICC's Right to Information and Information Privacy process;

g) A person must ensure they comply with section 45 of the *Invasion of Privacy Act 1971* in communicating or publishing the contents or a summary of a recorded private conversation to a member of the public or any third party entity (including Council contractors). Pursuant to section 45(1), it is an offence for a person to communicate to another person or publish any record or statement of a private conversation they were a party to and used a listening device to overhear, record, monitor or listen to, unless one of the following relevant exceptions contained within section 45(2) applies in the sense that it is:-

- made to another party to the private conversation;
- made with the express or implied consent of all parties to the private conversation;
- made in the course of legal proceedings;
- not more than is reasonably necessary in the public interest *or* in the performance of a duty of the person making the communication *or* for the protection of the lawful interests of that person; or
- made to a person who has, or is believed, on reasonable grounds by the person making the communication or publication to have such an interest in the private conversation as to make the communication or public reasonable under the circumstances in which it is made.

A "listening device" is defined as "any instrument, apparatus, equipment or device capable of being used to overhear, record, monitor or listen to a private conversation simultaneously with its taking place" (section 4 of the *Invasion of Privacy Act 1971*). A private conversation is defined as "any words spoken by one person to another person in circumstances that indicate that those persons desire the words to be heard or listened to only by themselves or that indicate that either of those persons desires the words to be heard or listened to only by themselves and by some other person, but does not include words spoken by one person to another person in circumstances in which either of those persons ought reasonably to expect the words may be overheard, recorded, monitored or listened to by some other person, not being a person who has the consent, express or implied, of either of those persons to do so" (section 4 of the *Invasion of Privacy Act 1971*).

If a person records a private conversation with a member of the public or a third party entity (including a Council contractor) which they anticipate will need to be published or communicated in any way, they should, wherever possible, ask all such persons for their consent to make the communication or publication.

If the person refuses to provide the consent requested or if consent is not able to be obtained for whatever reason (e.g. because it was not known at the time of the recording that any communication or publication would be necessary), then the matter must be referred to a Manager for determination as to whether the communication or publication is necessary and if so, whether one of the exemptions contained within section 45(2) of the *Invasion of Privacy Act 1971* applies; and

h) A person must also ensure that any communication or publication of the contents of a recording or photograph complies with the Information Privacy Principles (IPPs) contained within the *Information Privacy Act 2009*.

Record keeping responsibilities

1.2. All persons subject to this Policy must also comply with the following record keeping responsibilities:

a) All photography or recordings taken during work hours or within MICC facilities and held on a device by the person belong to MICC and that person transfers all rights and interests to MICC;
b) Persons should ensure that any recording created or received on a device is transferred as a compressed version of the original recording (preserving adequate quality) to the MICC Document Management System filed under confidential human resource documents as soon as practicable;
c) The original photographs or recordings are to remain unmodified and stored permanently on MICC Document Management System;
d) Persons who copy and edit recordings or photographs on a device must reintroduce those documents back in to MICC's Document Management System linked to the original file; and
e) In the event that a recording or photograph becomes corrupt for any reason and is therefore not available in Councils' archives, the person must prepare a file note stating this information and save the file note to the original file for future reference.

Additional responsibilities

1.3. In addition to the above responsibilities, the parties identified below must observe the following;

Chief Executive Officer	• Ensure that the policy is implemented consistently and fairly across the organisation; • Provide adequate resources for education, training, counselling and the other requirements of the policy.
Directors	• Direct the implementation of this policy within the department; • Enforce compliance with established procedures to safeguard sensitive and personal information.
Managers	• Manage the implementation of the policy within the section including holding discussions with employees regarding electronic recording as outlined in this policy.
Coordinators / Seniors / Team Leaders	• Implement the policy within the work area; • Support the managers in identification of electronic recording noncompliance; • Implement any restrictions or reasonable adjustments within the work area as approved by the manager; • Maintain confidentiality.
Human Resources / Workplace Health & Safety Coordinator	• Support directors/managers and staff in the implementation of the policy and its review; • Participate in any noncompliance matters as per Councils' Performance and Misconduct Policy.
Employees/Contractors/Volunteers	• Inform supervisor of any potential electronic recording noncompliance; • Comply with policy at all times.

2. RESPONSIBILITIES IN RELATION TO BYOD USAGE

General Responsibilities

2.1. The following must be observed by all persons subject to this Policy:

a) A person must only use a BYOD for work purposes if an MICC device is not reasonably available for the work purpose for which the BYOD is to be used;
Examples: A person accessing work email from a BYOD whilst at home or away from their workstation; A person recording a meeting or taking a photograph where the person has no access to a MICC device capable of performing these tasks; A contractor carrying out MICC work and who does not have access to a MICC device for the particular work purpose.
b) Persons must not use their own USB drive for work purposes and must use a Council issued USB drive; and
c) Persons who copy and edit work related documents on a BYOD device must reintroduce those documents back in to MICC's Document Management System and save them to the original file.

2.2 Where contractors utilise their own device connected to the MICC network, approval must be given by a Director prior to commencement.

Additional Obligations regarding file sharing, use of wireless networks and lost or stolen BYOD

2.3. Persons are responsible for ensuring that MICC information is not shared with any other device. Preferably or whenever practicable, MICC data on a BYOD should only be accessed with the devices Bluetooth and/or Wi-Fi functionality switched off (flight mode).

2.4. A person must not connect a BYOD to an unsecured wireless network (including "mobile hotspot") when the device has MICC files on it.

2.5 If a person loses a BYOD for work purposes or the BYOD is stolen, they must immediately notify their Manager of the loss or theft. Council may request that all files, personal and work related, be wiped remotely from the device in these circumstances.

BYOD Approval Requirements for Employees

2.6. Employees must not use a BYOD for work purposes until an approval from the Chief Executive has been given. An approval must be obtained in respect of each new BYOD device (including each upgraded device) the employee proposes to use for work purposes.

2.7. The following approval process applies to all applications for an approval:

a) Employees who wish to apply for an approval to use a BYOD for work purposes must make a written application to the Chief Executive Officer;
b) The application to the Chief Executive Officer must state the type and model of the BYOD device for which the approval is sought, the reasons why the approval is sought and contain a supporting comment as to the reasons why the approval is required from the employee's Manager. In general an approval will not be granted for employees to use a BYOD to access and download MICC files (including confidential information) from the MICC domain/network and will only be granted for use of a BYOD for the following genuine MICC work purposes;
   i. to check work MICC email;
   ii. to search the internet for work purposes;
   iii. to make work-related calls and a limited number of personal calls (during work hours); and
   iv. to take photographs and make recordings in accordance with this Policy;
c) The application must also state if the employee wishes to use a BYOD device for a work purpose which is not listed in paragraph 2.7(b) and ensure that the supporting comment from the Manager states why the employee requires use of the BYOD for this work purpose.

d) All approvals issued by the Chief Executive Officer for use of BYODs for work purposes will be recorded in a register maintained by Human Resources.

Approval conditions

2.8. All approvals issued by the Chief Executive Officer will be subject to the following conditions which must be complied with by the employee at all times:
   a) The employee must only use the BYOD for the MICC work purposes for which the approval is granted;
   b) The employee will be wholly responsible for all costs associated with the device, including repairs, maintenance and upgrades;
   c) The employee must accept responsibility for the consequences of use of the device for work purposes. This can include a requirement that all files, personal and work related, be wiped remotely from the device in the event of loss or theft;
   d) The employee must ensure that all of the following security measures are in place for an approved BYOD device:-
      i. A password (or equivalent) locking functionality;
      ii. The password (or equivalent) must be enabled at all times;
      iii. Current virus and malware protection;
      iv. The capacity to be remotely located and the data on the device remotely wiped;
      v. All MICC data and information must be stored in a folder that has encryption capability and individual password protection. The password for the folder must be different to that of the device itself;
      vi. Software that securely wipes files;
   e) The employee must ensure that MICC data on a BYOD is only accessed with the devices Bluetooth and/or Wi-Fi functionality switched off (flight mode); and
   f) A BYOD must never connect to an unsecured wireless network when the device has MICC files on it.
   g) Employees must submit an approved BYOD to the Information Technology Department for removal of all MICC data from the device in the following circumstances:-
      i. Immediately prior to the employee selling or gifting an approved BYOD to any third party;
      ii. Where an employee no longer intends to use an approved BYOD (including for example, because they are upgrading to a new BYOD device); and
      iii. Immediately prior to the employee ceasing employment at MICC.

3. ENFORCEMENT

3.1. MICC reserves the right, at its discretion, to require employees to demonstrate that any electronic recording or photograph made by the employee or the use of a BYOD is being undertaken in accordance with the law, this Policy and other MICC policies. Where an employee is unable to reasonably satisfy MICC of this, MICC reserves the right to review an employee's Device to the extent necessary to ensure it is being used in compliance with the law, this Policy and other MICC policies.

3.2. MICC recognises the need to fully enforce the provisions of this Policy and the *Local Government Act 2009.* Users must therefore comply with the requirements of this Policy.

3.3 MICC reserves the right to prohibit any photography or recording for any reason or for no reason.

Consequences of Breach for Staff

3.4. MICC employees breaching this Policy may breach their responsibilities as a local government employee under section 13 of the *Local Government Act 2009*, including their responsibilities to implement Council's policies and ensure that their personal conduct does not adversely reflect on Council's reputation. A breach of this Policy may result in disciplinary action under Chapter 8, Part 3, Division 1 of the *Local Government Regulation 2012* including termination of the person's employment,

demotion (including a reduction in remuneration), a deduction from salary or wages, suspending the employee's employment, issuing a written warning or reprimand to the employee or removal of the employees access to all or part of MICC's Computer Network (whether permanently or on a temporary basis).

Consequences of Breach for Contractors

3.5 Any breach of this policy by MICC contractors may result in MICC taking action against the contractor, subject to the terms of the contract, including termination or non-renewal of contractual arrangements, suspension of contractual arrangements or in disconnection of the contractor's access to all part of MICC's Computer Network (whether permanently or on a temporary basis).

Consequences of Breach for Volunteers

3.6. Any breach of this policy by a Volunteer may result in the person's volunteer position in Council being terminated or suspended or or in disconnection of the volunteer's access to all part of MICC's Computer Network (whether permanently or on a temporary basis).

4. VARIATIONS

4.1 Due to the diversity and frequent release of new devices and technologies, MICC will continually review and re-evaluate the contents of this policy. Accordingly, this policy will be reviewed at least annually.

DICTIONARY

For the purpose of this policy;

WORD OR PHRASE	EXPLANATION
"recording or photograph"	refers to recording an individuals' likeness (e.g. image or picture) or voice using audio recording (e.g. a tape, digital recorder or cellular telephone), video recording (e.g. video cameras or cellular telephones), digital imaging (e.g. digital cameras or web cameras), or other technologies capable of capturing an image or audio data (e.g. Skype) or photography (e.g. cameras or cellular telephones).
"Device"	refers to a mobile device for storing and transferring digital information. Examples include portable USB or 'flash' keys, memory cards, smartphones, tablets, laptops, notebooks, personal digital assistants, MP3 players, iPods, rewritable CDs, e-readers and any other device with inbuilt accessible storage.

RELATED DOCUMENTS

1. Right to Information Act 2009 (Qld)
2. Information Privacy Act 2009 (Qld)
3. Invasion of Privacy Act 1971 (Qld)
4. Public Records Act 2002 (Qld)
5. Queensland Local Government Act 2009
6. MICC Code of Conduct for Employees
7. MICC Performance and Misconduct Policy

This policy also draws on the guidance on record keeping obligations for mobile and smart devices provided by Queensland State Archives (QSA).