| | |
|---|---|
| **Document name:** | Information and Communication Technology |
| **Document Type:** | Policy |
| **Document Number:** | |
| **Domain:** | Meli Kindergarten Services |
| **Regulation:** | National Quality Framework |
| **Regulatory Area:** | Quality Area 7 |
| **Version:** | 1.0 |
| **Document Status:** | Published |
| **Effective Date:** | 25/10/2023 |
| **Review Date:** | 25/10/2026 |
| **Approver:** | CEO |
| **Custodian:** | Executive Director Services |

## 1. Purpose

This policy will provide guidelines to ensure that all users of information and communication technology (ICT) at Meli Kindergartens (Meli) or on behalf of Meli:

- understand and follow procedures to ensure the safe and appropriate use of ICT, including maintaining secure storage of information
- take responsibility to protect and maintain privacy in accordance with the Meli's *Privacy and Confidentiality Policy*
- are aware that only those persons authorised by the approved provider are permitted to access ICT at the service
- understand what constitutes illegal and inappropriate use of ICT facilities and avoid such activities.
- understand and follow professional use of interactive ICT platforms, such as social media and other information sharing platforms.

## 2. Policy Statement

Meli is a Child Safe organisation and will not defend or support any individual who uses an ICT device for an unlawful purpose. Adults within the kindergarten environment **must not** use any personal device to record or take photos of children. Staff may only use their personal device(s) during a rostered break, and only in an area that is not used for the education and care of children. Any adult that witnesses any incidence or suspicion of inappropriate behaviour or becomes aware of the transmission of any illegal material, must report it immediately.

This policy must be read in conjunction with Attachment 2: Unacceptable and Inappropriate Use of Personal and/or Meli Provided ICT facility.

Meli is committed to:

- professional, ethical, and responsible use of ICT at the service
- providing a safe workplace for management, educators, staff, and others using the service's ICT facilities and information sharing platforms
- safeguarding the privacy and confidentiality of information received, transmitted, or stored electronically
- ensuring that the use of Meli ICT resources complies with all organisational policies, including the Staff Code of Conduct, and relevant government legislation

- providing management, educators and staff with online information, resources, and communication tools to support the effective operation of the service.

## 3. Scope

This policy applies to the approved provider or persons with management or control, nominated supervisor, persons in day-to-day charge, early childhood teachers, educators, staff, students, volunteers, at Meli. This policy does not apply to children.

This policy applies to all aspects of the use of Meli supplied and staff personal ICT devices, including:

- Smartphones and Smartwatches
- iPad/tablets
- desktop top computers, laptops/notebooks
- copying, saving, or distributing files
- electronic bulletins/newsletters and notice boards
- electronic mail (email) and instant messaging (SMS)
- file sharing and file transfer
- file storage (including the use of end point data storage devices)
- internet usage
- video conferencing, online discussion groups and chat facilities
- portable communication devices including mobile and cordless phones.
- printing material
- social media, blogs, and streaming media
- subscriptions to mailing lists or other like services
- viewing material electronically

## 4. Background

The ICT environment is continually changing and Meli is committed to evolving with the progress of technology for the benefit of children, their families, staff, and applicable stakeholders. However, Meli is a child safe environment with zero tolerance for any form of child abuse or maltreatment and will manage the use of ICT by all staff and applicable stakeholders accordingly.

Meli staff and stakeholders have access to a wide variety of technologies via fixed, wireless, and mobile devices that support the delivery of quality early childhood services. ICT is a cost-effective, timely and efficient tool for research, communication, and management of the service, and Meli will use ICT resources in accordance with its legal responsibilities in relation to information privacy, security and the protection of staff, families, and children.

State and federal laws, including those governing information privacy, copyright, occupational health and safety, anti-discrimination, and sexual harassment, apply to the use of ICT. Illegal and inappropriate use of ICT resources includes pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment (including sexual harassment, grooming, stalking and privacy violations) and illegal activity, including illegal peer-to-peer file sharing.

## 5. Definitions

The terms defined in this section relate specifically to this policy.

**Anti-spyware:** Software designed to remove spyware: a type of malware that collects information about users without their knowledge.

**Chain email:** An email instructing the recipient to send out multiple copies of the same email so that circulation increases exponentially.

**Cloud storage:** a cloud computing model that enables storing data and files on the internet through a cloud computing provider that you access either through the public internet or a dedicated private network connection.

**Computer virus:** Malicious software programs, a form of malware, which can spread from one computer to another through the sharing of infected files, and that may harm a computer system's data or performance.

**Cyber safety:** The safe and responsible use of technology including use of the internet, electronic media, and social media to ensure information security and personal safety. There are three main areas of risk to safety:

- Content: being exposed to illegal, inappropriate, or harmful material
- Contact: being subjected to harmful online interactions with other users (including bullying)
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

**Defamation:** To injure or harm another person's reputation without good reason or justification. Defamation is often in the form of slander or libel.

**Disclaimer:** Statement(s) that seeks to exclude or limit liability and is usually related to issues such as copyright, accuracy, and privacy.

**Electronic communications:** Email, instant messaging, communication through social media and any other material or communication sent electronically.

**Encryption:** The process of systematically encoding data before transmission so that an unauthorised party cannot decipher it. There are different levels of encryption available.

**Endpoint data storage:** Devices or internet based options capable of storing information/data, including but not limited to:

- Cloud storage
- laptops
- USB sticks, external or removable hard drives, thumb drives, pen drives and flash drives
- iPads, iPods, and other similar devices
- cameras with USB drive connection
- iPhones/smartphones
- PCI/PC Card/PCMCIA storage cards
- other data-storage devices (CD-ROM and DVD).

**Firewall:** The primary method of keeping a computer/network secure. A firewall controls (by permitting or restricting) traffic into and out of a computer/network and, as a result, can protect these from damage by unauthorised users.

**Flash drive:** A small data-storage device that uses flash memory and has a built-in USB connection. Flash drives have many names, including jump drives, thumb drives, pen drives and USB keychain drives.

**Information sharing platforms:** Describes the exchange of data between various organisations, people, and technologies This can include but no limited to Dropbox, Google Drive, SharePoint, Skype for Business, One Drive

**Integrity:** (In relation to this policy) refers to the accuracy of data. Loss of data integrity may be either gross and evident (e.g., a computer disk failing) or subtle (e.g., the alteration of information in an electronic file).

**Malware:** Short for 'malicious software.' Malware is intended to damage or disable computers or computer systems.

**Portable storage device (PSD)** *or* **removable storage device (RSD):** Small, lightweight, portable easy-to-use device that can store and transfer large volumes of data. These devices are either exclusively used for data storage (for example, USB keys) or are capable of multiple other functions (such as iPods and PDAs).

**Security:** (In relation to this policy) refers to the protection of data against unauthorised access, ensuring confidentiality of information, integrity of data and the appropriate use of computer systems and other resources.

**Social Media:** A computer-based technology that facilitates the sharing of ideas, thoughts, information, and photos through the building of virtual networks and communities**.** Examples can include but not limited to, Facebook, YouTube, WhatsApp, Facebook Messenger, TikTok and Instagram

**Spam:** Unsolicited and unwanted emails or other electronic communication.

**USB interface:** Universal Serial Bus (USB) is a widely used interface for attaching devices to a host computer. PCs and laptops have multiple USB ports that enable many devices to be connected without rebooting the computer or turning off the USB device.

**USB key:** Also known as sticks, drives, memory keys and flash drives, a USB key is a device that plugs into the computer's USB port and is small enough to hook onto a key ring. A USB key allows data to be easily downloaded and transported/transferred.

**Virus:** A program or programming code that multiplies by being copied to another program, computer, or document. Viruses can be sent in attachments to an email or file or be present on a disk or CD. While some viruses are benign or playful in intent, others can be quite harmful: erasing data or requiring the reformatting of hard drives.

## 6. Responsibilities

| RESPONSIBILITIES | Approved provider (Meli) and persons with management control | Nominated supervisor and persons in day-to-day charge | Early childhood teacher, educators, and all other staff | Parents/guardians | Contractors, volunteers, and students |
|---|---|---|---|---|---|
| **R** indicates legislation requirement | | | | | |
| Ensuring that the use of ICT complies with all relevant state and federal legislation *(refer to Legislation and standards),* and all service policies *(including Privacy and Confidentiality Policy and Code of Conduct Policy)* | **R** | √ | √ | √ | √ |
| Managing inappropriate use of ICT as described in *Attachment 2* | **R** | √ | | | |
| Providing suitable ICT facilities to enable early childhood teachers, educators, and staff to effectively manage and operate the service | √ | √ | | | |
| Ensuring staff do not use their personal devices to record or take photos of children, and immediately reporting any incidence of suspicious behaviour of a compromising nature *(National Law 167)* | **R** | **R** | **R** | √ | **R** |
| Authorising the access of early childhood teachers, educators, staff, volunteers, and students to the service's ICT facilities, as appropriate | √ | √ | | | |
| Providing clear procedures and protocols that outline the parameters for use of ICT facilities both at the service and when working from home *(refer to Attachment 1)* | √ | √ | | | |
| Embedding a culture of awareness and understanding of security issues at the service | **R** | **R** | √ | √ | √ |
| Identifying the professional development and training needs, additional to Meli's mandatory training, of early childhood teachers, educators, and staff in relation to ICT. | √ | √ | | | |
| Ensuring secure storage of all information at the service, including backup files *(refer to Privacy and Confidentiality Policy)* | **R** | √ | √ | | |

| | | | | | |
|---|---|---|---|---|---|
| Adhering to the requirements of the *Privacy and Confidentiality Policy* in relation to accessing information on the service's computer/s, including emails | **R** | **R** | **R** | | |
| Following procedures to minimise unauthorised access, use and disclosure of information and data, which may include limiting access and passwords, and encryption | **R** | √ | | | |
| Ensuring that the service's liability in the event of security breaches, or unauthorised access, use and disclosure of information and data is limited by developing and publishing appropriate disclaimers | **R** | √ | | | |
| Developing procedures to ensure data and information (e.g., passwords) are kept secure, and only disclosed to individuals where necessary | **R** | √ | | | |
| Being aware of the requirements and complying with this policy | **R** | **R** | **R** | √ | **R** |
| Appropriate use of endpoint data storage devices by ICT users at the service | **R** | √ | √ | √ | √ |
| Ensuring that all material stored on endpoint data storage devices is kept in a secure location | **R** | √ | √ | | √ |
| Ensuring that written permission is provided by parents/guardians for authorised access to the service's computer systems and internet by persons under 18 years of age (e.g., a student on placement at the service) | **R** | √ | | | √ |
| Encourage early childhood teachers, educators, and staff to<br>share (forward, re-post or re-tweet) official and authorised Meli posts, tweets, material, or comment without substantial or meaningful change, as part of showing their affiliation<br>or support for the organisation, using their personal social media profile. *(refer to Attachment 3)* | √ | √ | | | |
| Complying with all relevant legislation and Meli policies, protocols, and procedures, including those outlined in *Attachments 1* | **R** | **R** | **R** | √ | **R** |
| Reading and understanding what constitutes inappropriate use of ICT *(refer to Attachment 2)* | **R** | **R** | **R** | √ | **R** |
| Using Meli ICE facilities in accordance with the Staff Code of Conduct | √ | √ | √ | | √ |
| Maintaining the security of ICT facilities belonging to Meli and keeping allocated passwords secure, including not sharing passwords and logging off after using a computer | **R** | **R** | **R** | √ | **R** |
| Accessing accounts, data, or files on computers only where authorisation has been provided | | √ | √ | | √ |
| Co-operating with other users of ICT to ensure fair and equitable access to resources | √ | √ | √ | | √ |
| Requesting licensed computer software and hardware via Meli ICT, as required | √ | | | | |
| Ensuring no illegal material is transmitted at any time via any ICT medium *(refer to Attachment 2)* | **R** | **R** | **R** | √ | √ |
| Using email, messaging, and social media facilities for service-related and lawful activities only *(refer to Attachment 2)* | √ | √ | √ | √ | √ |
| Using endpoint data storage devices supplied by Meli for service-related business only, and ensuring that this information is protected from unauthorised access and use | | √ | √ | | √ |

| | | | | | |
|---|---|---|---|---|---|
| Notifying Meli ICT of any damage, faults, or loss of endpoint data storage devices | | R | R | | R |
| Using a USB or portable storage device in accordance with the Staff Code of Conduct and this policy | | √ | √ | | √ |
| Restricting the use of personal mobile phones to rostered breaks, and only used in areas outside of spaces being utilised for education and care of children | R | R | R | | R |
| Responding only to emergency phone calls when responsible for supervising children to always ensure adequate supervision of children *(refer to Supervision of Children Policy)* | √ | √ | √ | | √ |
| Ensuring electronic files containing information about children and families are always kept secure *(refer to Privacy and Confidentiality Policy)* | R | R | √ | | √ |
| Responding to a privacy breach in accordance with *Privacy and Confidentiality policy.* | R | R | R | | √ |
| Complying with the appropriate use of social media *(refer to Definitions)* platforms *(refer to Attachment 3)* | R | R | √ | | √ |
| Always complying with this policy to protect the privacy, confidentiality, and interests of Meli employees, children, and families | R | R | R | R | R |

## 7. Evaluation

To assess whether the values and purposes of the policy have been achieved, Meli will:

- regularly seek feedback from everyone affected by the policy regarding its effectiveness
- monitor the implementation, compliance, complaints, and incidents in relation to this policy
- keep the policy up to date with current legislation, research, policy, and best practice
- revise the policy and procedures as part of the service's policy review cycle, or as required
- notifying all stakeholders affected by this policy at least 14 days before making any significant changes to this policy or its procedures, unless a lesser period is necessary due to risk *(Regulation 172 (2))*
- notifying all stakeholders affected by this policy at least 14 days before making any significant changes to this policy or its procedures unless a lesser period is necessary due to risk *(Regulation 172 (2))*.

## 8. Attachments

- Attachment 1: Procedures for use of ICT at the service
- Attachment 2: Unacceptable/inappropriate use of ICT facilities
- Attachment 3: Social Media Guidelines

## 9. Related Documents

Meli Kindergarten Services:

- Staff Code of Conduct
- Child Safe Environment and Wellbeing Policy
- Interactions with Children Policy
- Supervision of Children Policy
- Governance and Management of the Service Policy
- Privacy and Confidentiality Policy
- Staffing Policy
- Curriculum Development
- Enrolment and Orientation
- Complaints and Grievances Policy
- Occupational Health and Safety Policy

- Meli Social Media Policy

## 10. Sources

- Acceptable Use Policy, DE Information, Communications and Technology (ICT) Resources: https://www.education.vic.gov.au/school/teachers/management/infrastructure/Pages/acceptableuse.aspx
- IT for Kindergartens: www.kindergarten.vic.gov.au

## 11. Legislation and Standards

Relevant legislation and standards include but are not limited to:

- Broadcasting Services Act 1992 (Cth)
- Charter of Human Rights and Responsibilities Act 2006 (Vic)
- Crimes Act 1958 (Vic)
- Classification (Publications, Films and Computer Games) Act 1995
- Commonwealth Classification (Publication, Films and Computer Games) Act 1995
- Competition and Consumer Act 2010 (Cth)
- Copyright Act 1968 (Cth)
- Copyright Amendment Act 2006 (Cth)
- Cybercrime Act 2001 (Cth)
- Education and Care Services National Law Act 2010
- Education and Care Services National Regulations 2011
- Equal Opportunity Act 2010 (Vic)
- Freedom of Information Act 1982
- Health Records Act 2001 (Vic)
- Information Privacy Act 2000 (Vic)
- National Quality Standard, Quality Area 7: Governance and Leadership
- Occupational Health and Safety Act 2004 (Vic)
- Privacy Act 1988 (Cth)
- Privacy and Data Protection Act 2014 (Vic)
- Protected Disclosure Act 2012 (Vic)
- Public Records Act 1973 (Vic)
- Sex Discrimination Act 1984 (Cth)
- Spam Act 2003 (Cth)
- Trade Marks Act 1995 (Cth)

## ATTACHMENT 1: PROCEDURE FOR USE OF MELI PROVIDED ICT RESOURCES AT MELI KINDERGARTENS

### Email usage

- Content of emails and email addresses must always be checked before sending.
- When sending emails to multiple recipients, care should be taken to avoid the inappropriate disclosure of email addresses to a whole group of recipients; blind copying (BCC) should be used where appropriate.
- Always include a subject description in the subject line.
- Create an email signature that identifies employee name, title, service name, service phone number and address
- Always include a disclaimer which is common to all users, on emails to limit liability.
- Be cautious about opening files or launching programs that have been received as an attachment via email from the email itself. Instead, save an attachment to disk and scan with anti-virus software before opening, and keep an eye out for unusual filenames.
- Never open emails if unsure of the sender.
- Check email accounts on a regular basis and forward relevant emails to the approved provider or appropriate committee members/staff.
- Remove correspondence that is no longer required from the computer quarterly.
- Respond to emails as soon as is practicable.
- Never send unauthorised marketing content or solicitation emails
- Be suspicious of clickbait titles.

### Digital storage of personal and health information

- Digital records containing personal, sensitive and/or health information, or photographs of children must be password protected and stored securely so that privacy and confidentiality is maintained. This information must not be removed from the service without authorisation, as security of the information could be at risk *(refer to Privacy and Confidentiality Policy).*
- Digital records containing personal, sensitive and/or health information, or photographs of children may need to be removed from the service from time-to-time for several reasons, including for:
    - excursions and service events *(refer to Excursions and Service Events Policy)*
    - offsite storage, where there is not enough space at the service premises to store the records.

  In such circumstances, services must ensure that the information is transported, managed, and stored securely so that privacy and confidentiality is always maintained.
- ICT users are not to view or interfere with other users' files or directories, knowingly obtain unauthorised access to information or damage, delete, insert, or otherwise alter data without permission.
- Ensure all material stored on an endpoint data storage device is also stored on a backup drive, and that both device and drive are kept in a secure location.

### Backing up data

Data backup is managed by Meli ICT Services who will:

- Develop a written backup plan that identifies:
    - What is being backed up
    - Where it is being backed up
    - How often backups will occur
    - Who oversees performing backups
    - Who oversees monitoring the success of these backups
    - How will backup drives be stored securely

### Password Management

The effective management of passwords is the first line of defence in the electronic security of an organisation. All staff must adhere to Meli ICT Services password requirements.

Users should always follow these principles:

- do not share passwords with anyone. If there is an issue that requires you to do so, remember to change the password immediately after the issue has been resolved.
- never use the same password for work accounts as the one you have for personal use (banking, etc.).
- do not write down passwords or include them in an email.
- do not store passwords electronically unless they are encrypted.
- never use the “remember password” feature on any systems; this option should be disabled
- Do not use the same password for multiple administrator accounts.

**Working from home**

When an approved provider, nominated supervisor, early childhood teachers, educators or staff members are working from home they must:

- use all Meli ICT resources provided in accordance with this Policy and the Staff Code of Conduct
- conduct a workstation assessment; taking reasonable care in choosing a suitable workspace, including ergonomics, lighting, thermal comfort, safety, and privacy
- ensure security and confidentiality of workspace, keeping private, sensitive, heath information, planning, educational programs, and children’s records confidential and secure at all times
- keep allocated passwords secure, including not sharing passwords and logging off after using a computer
- adhere to the *Privacy and Confidently Policy*
- report breaches to privacy or loss of private, sensitive, and heath information to nominated superiors as soon as possible.

## ATTACHMENT 2. UNACCEPTABLE AND INAPPROPRIATE USE OF PERSONAL AND MELI PROVIDED ICT FACILITIES

**Meli Provided ICT Facilities**

Users of the ICT facilities (such as the internet, email, and social media) provided by Meli must not:

- create or exchange messages that are offensive, harassing, obscene or threatening
- create, copy, transmit or retransmit chain emails, spam, or other unauthorised mass communication
- use the ICT facilities as a platform to gain unauthorised access to other systems
- conduct activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules/discriminates against others based on race, nationality, creed, religion, ability/disability, gender, or sexual orientation
- use the ICT facilities to access, download, create, store, or distribute illegal, offensive, obscene, or objectionable material (including pornography and sexually explicit material).
- use the ICT facilities to make any personal communication that could suggest that such communication was made in that person's official capacity as an employee or volunteer of Meli
- conduct any outside business or engage in activities related to employment with another organisation
- play games
- use the facilities to assist any election campaign or lobby any government organisation
- exchange any confidential or sensitive information held by Meli unless authorised as part of their duties
- publish the service's email address on a 'private' business card
- harass, slander, intimidate, embarrass, defame, vilify, seek to offend, or make threats against another person or group of people
- breach copyright laws through making copies of, or transmitting, material or commercial software.

**Personal Devices**

All adults, including staff, volunteers, students, parents/carers of children and onsite contractors, attending a Meli kindergarten space must not:

- Using any form of personal recording device for any purpose in any area that is used for education and the care of children. Staff may only use a personal device during a rostered break, and only in an area that is **not** used for education and the care of children.
- Use a personal device to record or take photos of children. Any adult that witnesses suspicious or inappropriate behaviour at any Meli site must report it immediately to the kinder leader, or person in charge, or a trusted worker.
- Transmit any illegal material at any time via any ICT medium

**Breaches of this policy**

Meli will not defend or support any individual who uses an ICT device for an unlawful purpose.

- Individuals who use ICT at any Meli service for unlawful purposes may be liable to criminal or civil legal action. This could result in serious consequences, such as a fine, damages and/or costs being awarded against the individual, or imprisonment.
- Meli has the right to block access to internet sites where inappropriate use is identified.
- Employees who fail to adhere to this policy may be liable to counselling, disciplinary action or dismissal.
- Management, educators, staff, volunteers, and students who fail to adhere to this policy may have their access to the service's ICT facilities restricted/denied.

**Category 1: Illegal — criminal use of material**

This category includes but is not limited to:

- child abuse material offences relating to child pornography covered by the Crimes Act 1958 (Vic). 'Child abuse material' is defined in section 51A of the Crimes Act 1958 (Vic)
- objectionable material — offences relating to the exhibition, sale and other illegal acts relating to 'objectionable films' and 'objectionable publications' covered by the Classification (Publications, Films

and Computer Games) (Enforcement) Act 1995 (Vic). Such material has or would attract a classification of X18+ (restricted) or RC (refused classification) under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth)
- reckless or deliberate copyright infringement
- any other material or activity that involves or is in furtherance of a breach of criminal law

**Category 2: Extreme — non-criminal use of material**

This category includes non-criminal use of material that has or may attract a classification of RC or X18+ under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth).

This includes any material that:

- depicts, expresses, or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety accepted by reasonable adults to the extent that the material should not be classified
- describes or depicts in a way that is likely to cause offence to a reasonable adult or a person who is, or appears to be, a child under 18 (whether the person is engaged in sexual activity or not)
- promotes, incites, or instructs in matters of crime or violence
- includes sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults

**Category 3: Critical — offensive material**

This category includes other types of restricted or offensive material, covering any material that:

- has or may attract a classification of R18+ under the Guidelines for Classification of Films 2012, Guidelines for the Classification of Computer Games 2012 or National Classification Code scheduled to the Classification (Publications, Films and Computer Games) Act 1995 (Cth). Material may contain sex scenes and drug use that are high in impact
- includes sexualised nudity
- involves racial or religious vilification
- is unlawfully discriminatory
- is defamatory
- involves sexual harassment or bullying

**Category 4: Serious**

- This category includes any use which is offensive or otherwise improper.
- The categories do not cover all breaches of this policy. Matters not covered by the above categories will be dealt with on an individual basis and on the relevant facts.

## ATTACHMENT 3. SOCIAL MEDIA AND INFORMATION SHARING PLATFORM GUIDELINES

The below directives are essential to the safety and wellbeing of staff, children, and their families, and to ensure that Meli operates in a professional and appropriate manner when using social media and/or information sharing platforms.

Staff must exercise extreme caution using ICT facilities when accessing social media and/or information sharing platforms, whether in the workplace or relating to external events or functions involving Meli.

It is a breach of confidentiality and privacy to make posts or comments about children, families, staff, or management from Meli on social media sites without consent or authorisation. It is also an offence under current legislation, to record or use a visual image of a child, including transmitting the image on the internet, without the written consent of the child's parent.

Meli specifically requires that, unless you have the express permission, you:

- Do not video or photograph anyone, or post photos or personal details of other Meli staff, children, or families;
- Do not post photos or videos of Meli staff, children, or families on your personal Facebook page, or otherwise share photos or videos of staff, children, or families through social media;
- Do not create a Meli branded Facebook page, or other pages or content on social media that represents Meli, its staff, children, or families without authorisation from the approved provider;
- Do not post anything that could embarrass or damage the reputation of Meli, colleagues, children, or families.

**Staff must not:**

- post or respond to material that is, or might be construed as offensive, obscene, fraudulent, defamatory, threatening, harassing, bullying, discriminatory, hateful, racist, sexist, infringes copyright, constitutes a contempt of court, breaches a Court suppression order, or is otherwise unlawful or inaccurate;
- make any comment or post any material that might otherwise cause damage to Meli reputation or bring it into disrepute;
- imply that they are authorised to speak as a representative of Meli, or give the impression that the views expressed are those of Meli , unless authorised to do so
- use a Meli email address or any Meli logos or insignia that may give the impression of official support or endorsement of personal comments;
- use the identity or likeness of another employee, contractor, or other member of Meli;
- use or disclose any confidential information or personal information obtained in the capacity as an employee/contractor of Meli; or
- access and/or post on personal social media during paid workhours.

**Personal use of social media**

Meli recognises that staff may use social media in a personal capacity. This policy is not intended to discourage nor unduly limit staff using social media for personal expression or other online activities in their personal life.

However, staff should be aware and understand the potential risks and damage to Meli if they can be identified as an employee of Meli on social media, even if their activity takes place outside working hours or on devices not owned by Meli.

If an individual can be identified as an employee of Meli on social media, that employee must:

- only disclose and discuss publicly available information
- ensure that all content published is accurate and not misleading and, complies with all relevant policies of Meli
- expressly state on all postings (identifying them as an employee of Meli) the stated views are their own and are not those of Meli;
- be polite and respectful to all people they interact with;
- adhere to the Terms of Use of the relevant social media platform/website, as well as copyright,

- abide by privacy, defamation, contempt of Court, discrimination, harassment, and other applicable laws;
- ensure that abusive, harassing, threatening, or defaming postings which are in breach of Meli policies may result in disciplinary action being taken, even if such comments are made using private social networks outside of working hours.
- notify the approved provider or person with management or control if they become aware of unacceptable use of social media as described above.

**Consequences of unacceptable use of social media**

- Meli will review any alleged breach of this policy on an individual basis. If the alleged breach is of a serious nature, the person shall be given an opportunity to be heard in relation to the alleged breach.
- If the alleged breach is clearly established, the breach may be treated as grounds for dismissal. In all other cases, the person may be subject to disciplinary action in accordance with Meli *Code of Conduct Policy*.
- Meli may request that any information contained on any social media platform that is in breach of this policy be deleted.
- Meli may restrict an employee's access to social media on Meli ICT facilities or if they are found to have breached this policy or while Meli investigates whether they have breached this policy.