ABN 86 800 958 958

INFORMATION HANDLING PROCEDURE OF THE MONASH GRADUATE ASSOCIATION INC.

PROMULGATED ON 8 June 2020

Table of Contents

monash graduate association

ABN 86 800 958 958

INFORMATION HANDLING PROCEDURE

1. Short Title

These procedures may be cited as the Information Handling Procedure of the MGA.

2. Application

This procedures support the Monash Graduate Association's (MGA) in the protection of privacy and in its management of data breach incidents. These procedures apply to the MGAEC, MGA Council members and MGA staff its agents and contractors.

3. Objective

This procedure is created to enable the MGA to adopt best practice in handing private information aligned with the Australian Privacy Principles and the Privacy Act 1988. This procedure is created to support the Privacy Regulations of the MGA.

4. Authorising Provisions

4.1. This procedure is made pursuant to the Associations Incorporation Reform Act 2012 (Vic) and are subject to the MGA Constitution.
4.2. This procedure is created for the MGA to satisfy its obligations under the Privacy Act 1988 (Cth).

5. Purpose

The purpose of this response procedure is to provide guidance and instruction to all MGA staff regarding the safe and secure handling of personal and sensitive information.

6. Variation

MGAEC may amend these regulations in accordance with the provisions of the MGA Constitution.

7. Legal Responsibility

7.1. The MGA has a legal responsibility to take all reasonable steps to establish and maintain practices, procedures, and systems which comply with the APP.
7.2. The MGA has a legal responsibility to protect the privacy and confidentiality of individuals.
7.3. The MGA is bound by mandatory legislative reporting requirements

8. MGA Commitment

8.1. The MGA handles information of a personal and sensitive nature provided on confidential terms, including but not limited to physical and mental health, disability, family violence, criminal offences, and legal disputes and complaints. Such information can have serious consequences if not effectively managed.
8.2. The MGA recognises that the privacy of its constituents and that the risk of data breach exists within its everyday operations. The consequences of a data breach can be severe for its victims and requires ongoing risk assessment and management.

9. Mandatory Training

9.1. All MGA staff must, within six weeks of commencement, receive training in relation to privacy and handling of personal information at the MGA.
9.2. Training must be delivered by an officer of the MGA as stipulated by the Senior Advocate.

10. Staff Responsibilities

10.1. MGA staff must adhere to the Privacy Regulations of the MGA and:
  10.1.1. Treat all information confidentially, and not share any such information with unauthorised third parties;
  10.1.2. Only access information where required to perform regular duties;
  10.1.3. Avoid sharing and discussing information of others where not related to performance of duties and responsibilities;
  10.1.4. Take reasonable steps to avoid the misuse of information or a breach of privacy.
10.2. Where information relates to advocacy matters:
  10.2.1. All MGA staff must refrain from talking about student cases in public spaces.
  10.2.2. MGA Advocates must meet with students in enclosed rooms for privacy.
  10.2.3. Computer screens should be hidden from public view.
  10.2.4. Emails sent for advocacy purposes must contain a privacy clause to notify recipients of the confidential nature of emails received.

11. Storage of Digital Files

11.1. Digital files on portable devices must be stored in a locked cabinet or drawer that is not accessible to the general public.
11.2. Digital files stored on servers must be protected by appropriate security measures such as encryption and user access control.
11.3. Data collected for advocacy purposes must only be used and shared by advocacy staff.

12. Storage of Physical Files

12.1. Documents containing personal and/or sensitive information must be:
  12.1.1. stored in locked containers such as drawers or filing cabinets;
  12.1.2. stored indoors in a secure location not accessible by the general public;
12.2. Staff members are to refrain from taking physical files containing personal or sensitive information out of the MGA office when possible, and to use electronic access options where available.

13. Access Restrictions

13.1. Personal files are only to be accessed by staff where it is necessary for the fulfilment of their responsibilities.
13.2. Where a staff member ceases to have responsibility requiring access to personal information (for example, ceases to be an employee, transfers into a different role), they must transfer and remove all personal and sensitive information from their access. Their access to systems must be cancelled and revoked within 24 hours of departure.

13.3. Staff must store all personal and sensitive information relevant to their professional responsibilities on the secure Monash server or ChilliDB server, protected by identity management and authentication processes.

13.4. Staff must not use unsecure means such as USBs, or private hard-drives to store electronic data containing personal or sensitive information.

14. Off Site Access

14.1. This section covers working-from-home, and working at other campuses that are not the MGA Monash Clayton or the Monash Caulfield office.

14.2. Where a staff member must take physical files containing personal or sensitive information out of the MGA office, they must take all reasonable steps to make sure that the physical files cannot be accessed by others. This includes but is not limited to ensuring:

14.2.1. That files are secure in a closed bag or carry case;

14.2.2. Not to leave files unattended at any time;

14.2.3. That files are not placed where it is easily accessible by others; and

14.2.4. To avoid perusing files in public spaces (such as cafes or libraries) where others can observe the contents of the files.

14.3. Where a staff member accesses personal information via a mobile device, they must ensure that reasonable steps are taken to avoid unauthorised persons from viewing or accessing the information.

14.3.1. Avoiding accessing information in public spaces (such as cafes or libraries)

14.3.2. Ensuring to use secure and official apps to access content (e.g. my.monash, gmail)

14.3.3. Utilise official Monash equipment protected by Monash ICT measures (such as laptops) wherever possible.