Data Breach Policy

September 2018

Rationale

OLMC is responsible for the security, integrity and confidentiality of all the data it holds. Under the *Privacy Act 1988* (Cth), the College is obliged to have in place reasonable security safeguards to protect the personal information the College holds from interference and loss, and from unauthorised access, modification or disclosure.

Under the *Privacy Amendment (Notifiable Data Breaches) Act 2017,* which came into effect in February 2018, the College must be prepared to act quickly in the event of a data breach (or suspected breach). Individuals affected by the breach must be notified, and, in certain types of data breaches, the Office of the Australian Information Commissioner (OAIC) must also be notified. In addition, the College is required to have in place a Data Breach Response Plan for managing data breaches.

This policy outlines the processes to be followed by OLMC staff, students and/or parents in the event that they experience a data breach or suspect that a data breach has occurred. The policy applies not only to College community members but also to temporary staff, contractors and service providers working for and on behalf of OLMC.

Principles

- OLMC takes seriously its legal and ethical obligations to suitably protect the personal information it collects, holds, processes and shares. Every care is taken to protect personal data from breach incidents (either accidentally or deliberately).
- Compromise of personal information may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance and/or financial costs. As such, strong security measures are essential.
- OLMC is committed to maintaining a suitable set of controls – policies, procedures, systems, organisational structures, software and hardware functions – to ensure that specific security objectives are met. These controls are monitored, reviewed and improved, where necessary.
- In the event of a data breach or suspected breach, actions to reduce the harmful impacts of the breach will be a priority. The College has in place a Data Breach Response Plan and a Data Breach Response Team. The Team will ensure that prompt, remedial action is taken as soon as practicable after a breach, including mitigating potential harm to the person(s) affected.
- Individuals affected by a data breach at the College will be informed without undue delay. Depending on the nature and extent of the breach, the Office of the Australian Information Commissioner (OAIC) will also be notified.
- All OLMC staff, students and parents share responsibility for upholding the College's Privacy Policy and for the responsible use of the College's information systems, inclusive of information security. The prompt notification to the ICT Coordinator of suspected or actual data breaches is therefore expected of all staff, students and parents.

Definitions

Data Breach

A data breach is any event that has caused or has the potential to cause unauthorised access to personal information held by the College in any format. A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Examples of data breaches include:

- the disclosure of confidential data to unauthorised individuals;
- loss or theft of portable devices or equipment containing identifiable personal, confidential or sensitive data;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- suspected breach of the College's IT security and Acceptable Use policies;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- records altered or deleted without authorisation from the data 'owner';
- viruses or other security attacks on IT equipment systems or networks;
- breaches of physical security, e.g. forcing of doors or windows into a secure room or filing cabinet containing confidential information;
- confidential information left unlocked in accessible areas;
- insecure disposal of confidential paper waste;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- publication of confidential data on the Internet and social media sites;
- accidental disclosure of passwords;
- inadequate de-commissioning of office furniture (e.g. filing cabinets);
- misdirected emails or faxes containing identifiable personal, confidential or sensitive data.

Harm

Harm refers to the potential or actual impacts of a data breach on individuals, whether it is harm to their physical or mental wellbeing, financial loss, or damage to their reputation. Harm also refers to the potential or actual impacts of a data breach on the College's reputation and/or information assets.

Examples of harm include:

- Emotional and psychological harm
- Threats to an individual's physical safety
- Damage to reputation or relationships (individual and/or College)
- Loss of business or employment opportunities
- Identity theft
- Financial loss (individual and/or College).

Serious harm includes any of the examples listed above (physical, psychological, emotional, financial and reputation) where the impacts are deemed to be significant and/or severe.

Notifiable Data Breaches Scheme

The Notifiable Data Breach Scheme (NDBS) commenced in February 2018 following the enactment of the *Privacy Amendment (Notifiable Data Breaches) Act 2017.* The NDBS scheme requires entities covered by the Act to notify not only individuals affected by the breach but also the Australian Information Commissioner (OAIC) when and where a data breach is likely to result in serious harm to the individuals affected.

Personal Information

Personal information is information about an identified individual, or an individual who is 'reasonably identifiable'. Information that is not about an individual on its own can become personal information when it is combined with other information and this combination results in an individual becoming 'reasonably identifiable'.

Procedures

Preventative Practices

Staff and students are expected to be mindful of practices which may cause a data breach, such as:

- loss of portable devices or equipment containing identifiable personal, confidential or sensitive data;
- unauthorised use of information;
- a breach of the College's IT security and Acceptable Use policies;
- confidential information left unlocked in accessible areas;
- leaving IT equipment unattended when logged-in to a user account and failing to lock the screen to stop others accessing information;
- publication of confidential data on the Internet and social media sites;
- accidental disclosure of passwords;
- misdirected emails containing identifiable personal, confidential or sensitive data.

At all times, staff and students are urged to exercise due care and diligence in relation to these matters.

Incident Alerts

Where a data breach is known to have occurred (or is suspected) by any member of the College community, or by OLMC's contractors and service providers, the person(s) who becomes aware of this must in the first instance alert the ICT Coordinator and/or a member of the College Leadership Team.

The alert can be in person or via phone and include when the breach occurred or was first suspected (time and date); a description of the breach or suspected breach; the type of personal information involved; cause of the breach (if known); how it was discovered; which system(s) if any are affected (if known); and whether corrective action has occurred to remedy or ameliorate the breach (or suspected breach).

Data Breach Response Team

OLMC's Data Breach Response Team is responsible for carrying out the actions that reduce the potential impact of a data breach and that achieve a resolution to the cause and impacts of the breach. The Data Breach Response Team includes the following staff:

- The Principal (Chair)
- The ICT Coordinator
- The Business Manager
- The Network Manager

Depending on the nature and extent of the breach, other staff and external consultants may be co-opted, such as a media/communications advisor, lawyer, cybersecurity expert or ICT forensics consultant.

The Team will be guided by a four-steps response process specified in the *OLMC Data Breach Response Plan* (August 2018). These steps are:

1. Containing the breach
2. Assessing the breach
3. Notifying affected individuals and relevant authorities
4. Preventing future breaches.

As part of the Team's management of the incident, improvements to data protection policies, procedures, systems and technologies will be identified.

Related College Policies

- Mercy Education Limited and OLMC *Privacy Policy*
- *Student Responsible Use of Digital Technologies, Devices and Social Media Policy*
- *Staff Responsible Use of Digital Technologies Policy*
- *Staff Acceptable Use of Social Media Policy.*

Relevant Legislation and Resource Guides

- *Privacy Act 1988* (Cth)
- *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth)
- *Australian Privacy Principles*, Schedule 1 of the *Privacy Act 1988* (Cth)
- *OLMC Critical Incident Management Plan*
- *OLMC Data Breach Response Plan* (August 2018)
- Office of the Australian Information Commissioner, *Data Breach Preparation and Response Plan*, February 2018

Policy ratified: September 2018

Next Review Date: Twice annually – May 2019, September 2019

Persons responsible: The Principal and ICT Coordinator