Information Technology (IT)

Information Privacy and Security Policy

Policy Classification	-	**Information Technology**
Policy N°	-	**POL/514**
Policy Status	-	**Final**
Responsible Service Unit	-	**Information Technology**
Authorised by	-	**Executive Management Team (EMT)**
Date Adopted	-	**30 October 2016**
Next Review Date	-	**30 October 2017**

This policy is part of a suite of policies adopted by MCC or the Executive Management Team (EMT).

New or replacement policies can be created and developed within Service Units but can only be added to MCC's Policy Register by Governance Services following the approval of the policy by MCC or the EMT.

1. PURPOSE

The purpose of this *Information Privacy and Security Policy* is to meet Manningham City Council (MCC)'s obligations under the (*Privacy and Data Protection Act 2014 (Vic))* (the Act) with regards to the collection, management, and disclosure of Personal Information.

The responsible handling of Personal Information is a keystone to good corporate governance. MCC is committed to full compliance with its obligations under the Act and the Information Privacy Principles contained within the Act.

2. APPLICATION

This policy applies to all persons using IT products and services provided by MCC, including:

- employees
- contractors
- volunteers and
- persons employed by a third party agency.

This policy does not apply to Councillors.

3. DEFINITIONS

For the purpose of the policy the following definition applies.

Personal Information - Information about an individual whose identity is apparent or can reasonably be identified from that information (E.G: The name and address of a ratepayer or occupier).

Sensitive Information - Includes but not limited to information / opinion about an individual's racial or ethnic origin, political opinions, trade union membership, philosophical or religious beliefs, gender identity, sexual orientation, criminal record, or health information.

Unique Identifier - An identifier assigned by an organisation to an individual uniquely to identify that individual for the purposes of the operations of the organisation. In most cases this will be a number. This does not include identifiers that consist only of the individual's name.

User is used as a generic term meaning all persons using IT products and services provided by MCC to whom this policy applies as per section 2.

Worker is used as a generic term meaning all persons to whom this policy applies as per section 2.

Line Manager is used as a generic term meaning the person to whom the User directly reports to, who is an employee of MCC and who is of the level of Coordinator or above.

IT Equipment is used as a generic term meaning any Information Technology (IT) related equipment, IT device, IT peripheral, printer, notebook, laptop, server, windows tablets, multi-functional devices or desktop which are provided to the User by MCC or owned by MCC.

Communication Device is used as a generic term meaning any mobile phone, two-way communication radios, non-windows tablets and fax machines provided to the User for MCC business use or owned by MCC.

Application is used as a generic term meaning any MCC licensed software, application or database to which Users have access to perform their day to day activities.

SAM (Software Access Manager) is a tool used by IT for managing User's access to MCC Applications.

4. PRIVACY PRINCIPLES AND GUIDELINES

MCC complies with the ten Information Privacy Principles (IPPs) contained within the Act. The ten principles and the controls in place at MCC to comply with the IPPs are defined below:

4.1 Collection (IPP 1)

MCC will only collect Personal Information and Sensitive Information for a lawful purpose. Forms used by MCC for the collection of Personal Information must make reference to the Act. The forms must include:

- Why MCC is collecting Personal Information
- How the information may be accessed
- The purpose for collecting the information
- With whom MCC shares the information.

The following privacy statement must be included on any document which is used to collect forms used to capture and collect Personal Information:

"Manningham City Council is committed to full compliance with its obligations under the Privacy and Data Protection Act 2014 (Vic) and the Health Records Act 2001 (Vic). All Personal Information collected by MCC will be used for MCC's business purposes and kept confidential. It will not be disclosed to third parties unless MCC is required to disclose the information under other legislation or disclosure is necessary to complete the purpose for which it is sought. You may access information you have provided to MCC at any time and make corrections if you believe that information is incorrect. Copies of MCC's Information Privacy and Security Policy and Health Records Policy are available on the website at www.manningham.vic.gov.au/privacy."

4.2 Use and Disclosure (IPP 2)

MCC must not use or disclose Personal Information within MCC, or disclose it outside MCC, for a purpose other than:

- The primary purpose for which it was collected;
- A directly related secondary purpose where the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;

- In accordance with legislative requirements;
- For another purpose where the individual concerned has consented; or
- Where it is considered reasonable to do so. (e.g. ownership details under the Fences Act 1968 Part 1 Section 9 (1)(b)).

Organisations to which MCC may disclose Personal Information include: the Ombudsman, debt collection agencies, insurers, legal advisors, contracted service providers, printer and mailing services, State Government agencies, law enforcement bodies and courts.

If Personal Information regarding a Worker is requested, the information will be provided if authorised by the Worker in advance or MCC is required to by law.

In circumstances where the health or safety of a person is at risk, MCC reserves the right to disclose Personal Information without consent if deemed reasonable.

4.3 Data Quality (IPP 3)

MCC will endeavour to ensure that the Personal Information it collects, uses or discloses is accurate, complete and up-to-date.

4.4 Data Security (IPP 4)

To reduce the risk of unauthorised disclosure all papers containing Personal Information are required to be securely stored at all times. Personal Information about real people should not be used as training material.

4.5 Openness (IPP 5)

MCC's *Information Privacy and Security Policy* and associated privacy statement detail MCC's management of Personal Information. Both of these are available publically.

On request MCC will inform an individual in general terms on the types of Personal Information it holds and for what purposes and how it collects, holds, uses and discloses that information.

4.6 Access and Correction (IPP 6)

MCC must provide access to information held by MCC about an individual on request, except in specific circumstances as outlined within the Act.

Where MCC holds Personal Information about an individual and the individual is able to establish that the information is incorrect, MCC will take reasonable steps to correct the information.

In the event that MCC and an individual disagree about the veracity of Personal Information held by MCC, MCC will take reasonable steps to record a statement relating to the disputed information if requested by the individual.

Should an individual wish to access their Personal Information, they should contact MCC's Privacy Officer.

4.7 Unique Identifiers (IPP 7)

MCC will not assign Unique Identifiers to individuals unless the assignment of the identifier is necessary to perform any of MCC's functions or is required by law.

MCC will also not knowingly apply any Unique Identifier already in use by another organisation unless the individual consents to the use and disclosure or the conditions for use and disclosure set out in the Act are satisfied.

4.8 Anonymity (IPP 8)

Where lawful and practicable, MCC will provide a person with the option of not identifying themselves when supplying information or entering into transactions with it. However, anonymity may limit or hinder MCC's ability to process an application, request or complaint.

MCC reserves the right to take no action in any matter, within reason, if the relevant Personal Information is not submitted to MCC with the application, request or complaint.

4.9 Trans-border Data Flow (IPP 9)

MCC may transfer Personal Information outside of Victoria only if the data transfer conforms with the reasons and conditions outlined in the Act.

Some systems utilised by MCC may have data hosted by a third party outside of the state of Victoria. MCC will endeavour to ensure where possible data held externally is subject to similar or equal information privacy laws as Victoria.
The following notation should be included on online web forms used to capture and collect Personal Information hosted outside of Victoria:

> *"Manningham City Council is committed to full compliance with its obligations under the Privacy and Data Protection Act 2014 (Vic) and the Health Records Act 2001 (Vic)."*
>
> *"[INSERT SOFTWARE / PRODUCT NAME] is a cloud based software tool that is used to collect and temporarily store any information you complete on this form. This information is hosted in a data centre external to MCC's computer systems and is subject to not only Victorian legislation but also privacy legislation applicable to the location of the hosting data centre.*
>
> *All data hosted within the United States and its Territories or by US owned companies located worldwide may be accessed by the Federal Bureau of Investigation (FBI) without a court order and without permission from MCC under the provisions of the United States Patriot Act (2001)*
>
> *By clicking on the link to the form you consent to your information being collected and stored by [INSERT SOFTWARE / PRODUCT NAME] on behalf of Manningham City Council"*

4.10 Sensitive Information (IPP 10)

MCC will not collect Sensitive Information about an individual except for circumstances specified under the Act.

5. EXTERNAL CONTRACTORS

If a contractor breaches the IPPs the MCC will be held responsible unless the contractor has agreed to be bound by the IPPs in an enforceable contract with MCC. It is the intention of MCC to require contractors to comply with the IPPs and the provisions of the Act in all respects.

6. PUBLIC REGISTERS

Public registers kept pursuant to legislative provisions are available for limited perusal at MCC's Customer Service Desk. MCC will not provide copies of these registers. The only copying permitted is by hand transcribing by the person viewing the register.

7. NOTEBOOK SECURITY

Users are responsible for the security of their notebook and the information it contains. Users must avoid situations where theft of the notebook is possible. A notebook displaying Sensitive Information outside of MCC secure premises must be positioned so that the screen cannot be viewed by others.

To protect of the security of information on notebooks, all MCC notebooks are:

- Protected by a user name and password;
- Bitlocker encryption enabled;
- Fitted with additional security including bios passwords and settings that prevent the machine being booted up using alternative media; and
- Meet the MCC security requirements - e.g. anti-virus, personal firewall, patches are installed and maintained etc.

8. CYBER CRIME PREVENTION

- All Workers can log into MCC's intranet from any device outside of MCC via username and password authentication. All Workers must log out of the intranet when leaving the device, other than their MCC issued notebook, unattended.
- Workers must promptly inform the Information Technology (IT) Helpdesk about suspected information security problems including virus or malware infection, denial of service, loss or damage to equipment or social engineering attacks.
- If a security incident occurs, IT will take over to contain and eliminate the threat.
- Intrusion prevention systems and anti-virus software are installed to handle attacks entering MCC and remote connections are configured to securely authenticate Workers.
- A process is in place to disable Worker accounts upon leaving the organisation.
- Workers accessing the computer systems or networks of MCC are required to adhere to MCC policies and security requirements.

- Unless there is a legal or statutory requirement to disclose security incidents affecting its computer systems or networks, MCC does not publicise these incidents.
- If MCC experiences a cyber-crime incident an investigation is carried out to determine the cause and effect of the event.
- The Manager Information Technology is responsible for arranging regular comprehensive audits of the computer systems and networks by an independent auditor and present the report to the Audit Committee. The report must contain a detailed description of the security risks currently facing the organisation and recommendations for preventing or mitigating those risks.
- IT is responsible for developing and maintaining detailed procedural documentation to ensure that MCC can recover from any unforeseen event.
- Before mobile devices with networking capabilities are purchased for MCC a risk assessment must be carried out by the Helpdesk and Infrastructure Coordinator to confirm that these devices do not create additional security vulnerabilities which are unacceptable to MCC.
- Any attempt to interfere with, prevent, obstruct or dissuade a Worker who wants to report a suspected information security problem or breach of policy is strictly prohibited. Any form of retaliation against a Worker reporting or investigating information security problems is also prohibited.

9. HANDLING SECURITY INCIDENTS

- To ensure a quick, effective, and orderly response to an incident, documented procedures, including escalation procedures, must be followed by IT when a security breach is reported.
- A forced password change will be initiated if there has been a compromise or a suspected compromise of the computer systems or networks of MCC.
- If IT suspect that a security incident is malicious, care will be taken not to disturb or destroy the chain of evidence.
- Information describing all reported information security problems and incidents will be retained as required by legislation.

10. PRIVACY RELATED COMPLAINTS

- Individuals who feel aggrieved by MCC's handling of their Personal Information are encouraged to contact MCC's Privacy Officer. A written response to the complaint, will be made within 30 days of lodgement of the complaint. Alternatively, complaints may be made directly to the Privacy and Data Protection Commissioner. The Commissioner may decline to hear the complaint if the person has not first made a complaint to MCC.
- Where an individual who has requested information is aggrieved by the conduct of MCC in the following circumstances: (a) contravention of a privacy principle that applies to MCC and/or; (b) unwarranted disclosure of Personal Information kept in a public register, the individual may lodge a written complaint regarding MCC's conduct. All complaints must be in writing and addressed to:

Information Privacy Officer
Manningham City Council
P O Box 1
DONCASTER VIC 3108

- Complaints must be lodged within 6 months from the time the complainant first became aware of the conduct or misconduct. At all times the contents of the complaint will be kept confidential.
- All complaints lodged with MCC will be subject to a formal review to determine if a breach has occurred and if so the cause of the breach.
- Following completion of a review of the complaint, MCC will do one or more of the following: (a) make a formal apology to the complainant; (b) take appropriate remedial action; (c) take no further action; (d) provide undertakings that the conduct will not occur again and/or; (e) implement administrative measures to ensure that the conduct will not occur again.
- MCC will notify the complainant in writing of: (a) the findings and the reasons for those findings; (b) any proposed actions to be undertaken and; (c) the right of the applicant to have those findings and the MCC's proposed action, reviewed by the Victorian Civil and Administrative Tribunal.
- All enquiries regarding MCC's *Information Privacy and Security Policy* and the handling of Private Information within MCC should be directed to MCC's Information Privacy Officer.

11. POLICY BREACHES

- Workers who are in breach of this policy may have their IT access revoked.
- Employees who are in breach of this policy may be subject to disciplinary action, up to and including the termination of employment, in accordance with the *Disciplinary Policy* (POL/238).

12. SUPPORTING PROCEDURES AND POLICIES

- *Health Records Policy* (POL/488)
- *Records Management Policy* (POL/490)
- *Employee Code of Conduct* (POL/496)

13. RELATED LEGISLATION AND REFERENCES

Where the Act is silent on any particular aspect, reference shall be made to the *Privacy Act 1988 (Cth)*. If the Act is inconsistent with a particular piece of legislation, other legislation will take precedence. Other legislation, acts and standards under which MCC operates include, but are not limited to:

- ISO/IEC 27002:2007 (Information technology -- Security techniques -- Code of practice for Information Security Management).
- Electronic Transactions Act 2000

- Evidence Act 2008
- Freedom of Information Act 1982
- Health Records Act 2001
- Local Government Act 1989
- Public Records Act 1973
- Victorian Civil and Administrative Tribunal Act 1998

and a range of other instruments specific or related to regulatory or service provisions of Manningham City Council.