Platform Notifiable Data Breaches Scheme Statement

Effective from 1 February 2018. For more details, visit the Help Centre or contact us by phone on 1300 762 515 or email support@mycommunitydirectory.com.au

Your information is important to us and to the community and as custodians of this information, the Platform Administrators and Platform Providers take data management seriously. The Platform collects limited private information and limits its data collection to routine work personal information which does not require us to comply with the Notifiable Data Breaches (NDB) scheme under Part IIIC of the *Privacy Act 1988* (Privacy Act).

We understand the importance of transparent data management and have developed strategies to protect the information we hold and ways to reduce the risk of harm if the Platform is accessed by unauthorised users.

Protecting Your Information

The Platform software:

1. Uses industry standard security measures in data inscription to reduce the risk of a data breach
2. Uses password protection to restrict access to data when it is removed from the website.
3. Encourages the use of role-based access permissions and has created flexible options for Members to create and manage access permissions of staff
4. Restricts access to information based on the type of organisation, geography, class of service and your relationship with them.

The Platform environment:

1. Uses Microsoft Azure, secure and reliable hosting
2. Is based in Australia

Data Breach Plan

If we become aware of a data breach by us or our members we are committed to:

1. *Assessing the breach focusing on understanding how, when and why it happened.*

2. *Reacting to the breach by focusing on limiting its impact and reducing the risk and ongoing impact to our members*

3. *Notifying of the breach* if required and providing as much details as possible to members to assist them to respond.

4. *Reviewing our response to the breach* by focusing on how we assessed, reacted and notified of the breach and how we can strengthen our systems and processes to reduce the chance that we will have a data breach in the future.

What Personal Information May We Hold About You?

Information	Purpose	Protection
Title, First Name, Surname and Gender	Supports contact by agencies such as Councils and related community groups	Access restricted based on membership type, user role, geography and class of service
Work Address, Email, Phone, Mobile and Position (Job Title)	Supports contact by agencies such as Councils and related community groups	Access restricted based on membership type, user role, geography and class of service
User Name, Email, Phone, Mobile	Supports access to the platform and member communication	Access restricted to key organisations in your area (such as Council) and organisation administrators
User Password	Supports access to the platform	Stored encrypted and salted using a modern and secure standard encryption scheme
OAuth tokens	Allows login via social accounts such as Facebook, Google and Microsoft Passport	Related social credentials are not identifiable. These can be revoked on the third-party platform.
IP Address	Data analysis and reporting	Stored in a secure repository restricted to platform administrators. Information is aggregated and de-identified in reporting to other agencies.
Login History	Data analysis and reporting	Access restricted to key organisations in your area (such as Council) and organisation administrators
Search History (as a logged-in user only)	Data analysis and reporting	Access restricted to platform and organisation administrators