

# Privacy Policy

MCB International Pty Limited (ACN 149 360 743), trading as Consent2Go ("Consent2Go"), is an Australian owned and operated private entity, providing a software solution for schools, Consent2Go (the "Product"). This Policy provides guidance on collection, storage, security, and processing of data on Consent2Go.

In the Terms, 'Us', 'We' and 'Our' refers to MCB International Pty Limited trading as Consent2Go.

## Purpose of this Policy

The purpose of this document is to outline the data collected in the Product and inform users of their rights with respect to the handling of their data.

The Policy outlines:

- How the data is collected.
- The kinds of data collected.
- Strategies employed to ensure data is protected.
- Consent2Go's use of personal data.
- Consent2Go's processes in the event of a breach.

The Policy is written in accessible language to ensure that it can be readily understood by all relevant Product users. Users have the right, at any time, to seek clarity or further enquire into any provisions in this Policy.

## Scope and Application

This Policy applies to all information collected, stored and processed by the Product in the process of providing the Services.

The Policy also extends to the use of the Consent2Go website.

The scope of this Policy does not extend to third parties, such as linked sites within the Product. These links are provided for convenience and are not governed by Consent2Go's Privacy Policy.

## Consent

In any case where data collection requires consent, express or implied, Consent2Go will make all attempts to ensure that all required information provided to the user adequately outlines the choices available to you as an individual with regard to the handling of your data.

All end users providing consent to Consent2Go's handling of data must have the capacity to give consent. Consent must be informed, voluntary, specific, and current. If the consent provided does not meet these requirements, then Consent2Go will regard the consent as void. Examples of those unable to provide consent may include minors, those with serious mental or physical disabilities, those who are temporarily incapacitated, or have a limited understanding of English.

If there is doubt or confusion as to the capacity of an individual to provide consent, we encourage that individual to contact us and seek the appropriate support. Appropriate support may include, but is not limited to, a guardian, an individual with enduring power of attorney, an individual regarded as a 'responsible person' under relevant legislation, a nominated representative at a time where the individual was capable of providing consent, or an interpreter.

It is within the rights of the end-user to withdraw consent at any time. Consent2Go is committed to ensuring that the withdrawal of consent is an easy and accessible process. Consent2Go is contractually bound to provide this information to the school. If a user wishes to withdraw their consent, they must liaise with their school. The end user must be aware of the consequences of such withdrawal, including the loss of access to the Services.

## **Legislation**

Consent2Go understands our statutory obligations under relevant Australian law, including the Privacy Act 1988 (Cth) "Privacy Act" and takes active steps to ensure it is always compliant with all Australian Privacy Principles.

Consent2Go has a comprehensive Data Breach Plan that is compliant with the Notifiable Data Breaches Scheme pursuant to the Privacy Amendment (Notifiable Data Breaches Act) 2017.

Consent2Go is committed to maintaining the alignment of our business practices with all applicable legislation and ensures that this is done in a transparent and good-faith manner. Consent2Go ensures that all reasonable steps to review relevant legislation and update processes are undertaken on a rolling basis.

## **Notification of the Collection of Personal Information**

Consent2Go is committed to ensuring that all individuals are aware of the collection of personal information prior to, and at the time of collection. Consent2Go takes reasonable steps to ensure this is done in a transparent, good-faith manner.

All collection of personal information occurs on a voluntary basis through Profile Updates and Excursion Invites. The product ensures end-users are notified of the collection of personal information at the point of collection.

## **Methods of Data Collection**

Consent2Go ensures that all data collected from an individual is collected in a lawful and ethical manner and is collected from either the end-user or the school directly.

The Product has two main methods of data collection: the Excursion Invite and the Profile Update.

Data may also be collected through our website, including contact forms and cookies. In the event cookies are collected, all information collected will be de-personalised and aggregated.

## **Nature of Data Collected**

Consent2Go only collects the data necessary to provide the Services of the Product. The type of personal information collected by Consent2Go is, but not limited to:

- Name
- Contact details - mailing address, email address, telephone numbers
- Any additional information relating to you that you provide to us directly through the Product or indirectly via the school through your use of the Product
- Any other personal information that may be required to facilitate the services of the Product.

Consent2Go does not collect or store biometric data.

Consent2Go does not collect or store credit card information.

## **Data Usage, Processing and Handling**

As an information service provider, Consent2Go relies on accurate personal information to effectively provide the Services of the Product. Consent2Go collects personal information for the following reasons:

- To provide the Services offered by the Product.
- To verify your identity in data-related dealings to ensure data-protection.
- To ensure you are kept informed of any changes to the Services or this Policy in the future.

Without accurate personal information, Consent2Go is unable to provide the Services.

## **Unsolicited Information**

Consent2Go may, from time to time, be provided with unsolicited information by system users. In the event of receiving such information, Consent2Go will make a decision as to whether the data received may fall within the scope of Consent2Go's ordinary data collection. If the data does fall within the scope of the data collected in Consent2Go's business processes, the data will be retained and stored as per Consent2Go's processes. If the data does not fall within the scope of the data collected in Consent2Go's business processes, the data will be destroyed in a timely manner.

## **Data Security**

Consent2Go is committed to ensuring the security, integrity and privacy of all personal information collected by the Product. We take all reasonable steps to ensure that the personal information provided is safeguarded by the appropriate, best-practice security protocols. Consent2Go employs an advanced data classification policy to evaluate the sensitivity of personal information. Based on the outcome of the sensitivity evaluation, data is tagged and protected by role-based security, ensuring that access to Confidential or Highly Sensitive information is limited.

Employees employed by Consent2Go are trained in data security best-practice, and Consent2Go takes active steps to ensure that human interaction with data is minimised where possible.

Consent2Go does not actively use Contractors, however, we may employ unique specialist personnel for specific pieces of work. Consent2Go ensures the Contractors access to data is directly supervised and limited to the minimum amount required.

## **Anonymity and Pseudonymity**

Consent2Go requires the identity of system users in order to provide the Services and cannot provide the Services to an anonymised user.

## **Correcting your Personal Information**

Product users have a right to request a copy of their personal information, request to modify the information, or request an erasure or deletion of the data. To correct any data stored within in the Product, Consent2Go provides the technical means to ensure end-users can undertake a profile update at any time to modify, correct, and alter their record.

In instances where the provision of requested information may interfere with the rights, privacy, or freedoms, cause a breach in privacy or confidentiality, or violate any relevant laws, Consent2Go will decline the request and promptly provide reasons in writing for doing so.

## **Destruction of Personal Information**

Users have the right to request the removal of their personal information if they deem their personal information to be no longer required or wish to no longer be able to make use of the Services. If a user wishes to have their personal information removed from the Product, they must liaise with their school. If the user is no longer enrolled at their school, Consent2Go will assist with the removal of their personal information.

Users should be aware that there are cases where Consent2Go is unable to comply with this request for statutory reasons. If Consent2Go refuses the request for erasure or destruction, we will promptly provide a reason in writing for the refusal, with reference to the relevant legislation.

## Data Disclosure

Consent2Go will never sell or disclose your Personal Information to third parties unless required by law to do so. In the event Consent2Go is required by law to disclose such data, the end user whose data is affected will receive written notice from Consent2Go, unless this disclosure is also forbidden by law.

Consent2Go will never transfer or communicate your personal information through links to third-party sites on the product.

## Data Breach Protocol

In the event of a privacy breach, Consent2Go is committed to following the best practice guidelines outlined in the Office of the Australian Information *Commissioner's data breach preparation and response* guideline, the authoritative guideline on responding to a data compliant with the Privacy Act (Cth) 1988. Consent2Go's Data Classification Policy will be used to complement the assessment of breach severity in line with best practice.

In the event of a breach, Consent2Go will ensure the following is conducted:

- All necessary action has been undertaken to contain and control the breach.
- A comprehensive risk assessment of the breach is conducted, giving regard to:
  - The type of personal information breached, and its classification under Consent2Go's Data Classification Guideline.
  - The cause of the breach and the extent
  - The nature of the breach.
- All remedial action is taken to mitigate the severity of the breach.
- All relevant individuals and bodies are notified of the breach, including the Australian Privacy Commissioner.
- A review of data integrity processes is undertaken, ensuring necessary action to rectify the breach is undertaken, and ensure compliance with international best-practice.
- A prevention plan is in place to avoid a future incident.
- Policies and procedures are reviewed and updated with required security changes as required.
- Employees are trained and upskilled in data integrity practices as required.
- Where applicable, a review of service delivery partners involved in the breach is undertaken.

## Changes to this Policy

Although changes are likely to be minor, Consent2Go may change this Policy from time to time. Any changes are at Consent2Go's discretion, and users should routinely check this Policy for updates.

## Complaints

If you wish to make a complaint or enquiry regarding the handling of your personal information, please direct any concerns to [contactus@consent2go.com](mailto:contactus@consent2go.com)

## Definitions

---

**Data Breach** – A data breach (“Breach”) refers to any unauthorised access of personal information, unauthorised disclosure, or loss of data where such loss could increase the likelihood of the above.

**Confidential** – (“Confidential”) refers to data which, if breached, compromise the wellbeing of a Consent2Go customer in a way which does not necessarily present serious harm.

**End User** – (“End User”) refers to staff and parent/guardian users of the product.

**Highly Sensitive** – (“Highly Sensitive”) refers to data which, if breached, would compromise the safety of a Consent2Go customer or lead to another form of serious harm.

**Personal Information** - Consent2Go defines ‘personal information’ (“Personal Information”) in accordance with the [Australian Privacy Act \(Cth\) 1988](#). Under the Act, ‘personal information’ refers to a broad range of information which could lead to ascertaining the identity of an individual. The Act classifies personal information into two categories: personal and sensitive information. Consent2Go stores personal information, such as an individual’s name, address, contact information, and date of birth, and sensitive information such as health records. In order to safeguard all personal and sensitive information, Consent2Go operates under a complex data classification policy which assesses the sensitivity of data and assigns appropriate security protocols based on data sensitivity.

**Product** – (“Product”) refers to Consent2Go, the software solution provided by MCB International Pty Ltd trading as Consent2Go.

**Services** – (“Services”) refers to all the services and functionality provided by the Product.

**Website** – (“Website”) refers to the Consent2Go website.