Suttons

PRIVACY HANDBOOK

How to collect, store, and access customer details using Suttons authorised apps on your personal device

WHY IS THIS NON-NEGOTIABLE?

Under the Privacy Act 1988, Suttons is legally bound by Australian Privacy Principle 11 (APP 11), which requires us to take **reasonable steps** to protect the personal information we hold from misuse, interference, loss, and unauthorised access or disclosure. Allowing employees to store customer information in devices that are not authorised by Suttons would place the company in breach of the Privacy Act, as it would not be taking reasonable steps to protect that information. This action would expose you, personally, and Suttons, to significant penalties and regulatory action by the Office of the Australian Information Commission (OAIC) under the Statutory Tort for Serious Invasions of Privacy.

WHAT THIS MEANS FOR YOU IN PRACTICE

Authorised Company Platform

Customer data **must not** be stored on personal devices.

All Company data must be accessed and saved exclusively through Suttons-authorised platforms using company-issued login credentials. Approved platforms include (but are not limited to):

- Microsoft Outlook
- Business CRM applications (e.g. DealerSocket, Drive Expert)

Local storage, native device apps, camera rolls, contacts, downloads, or any offline saving to personal devices is strictly prohibited.

Correct Method

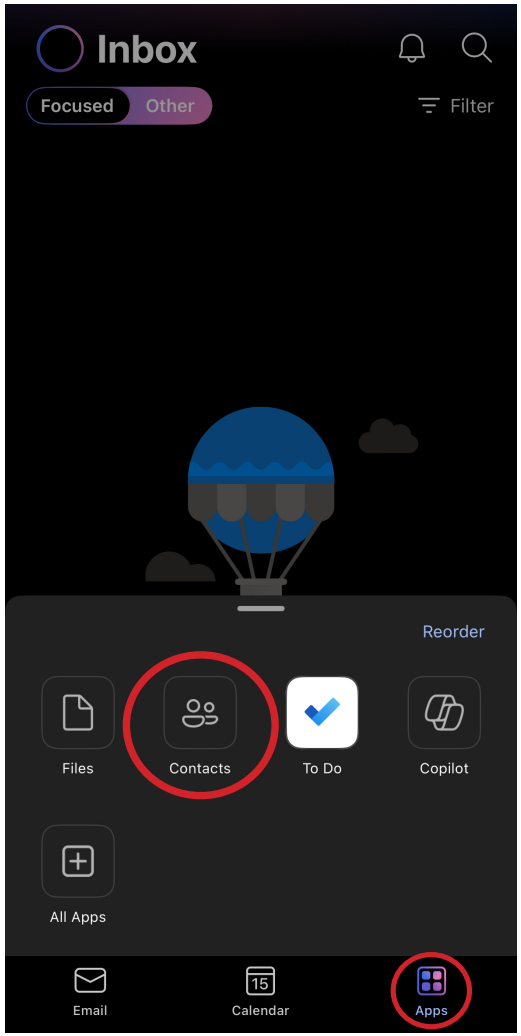
Install the official *Outlook* or *DealerSocket* app on your mobile device and log in with your Suttons credentials. This provides secure, encrypted access without creating an uncontrolled copy of the data on your personal device.

Personal Phones/Devices

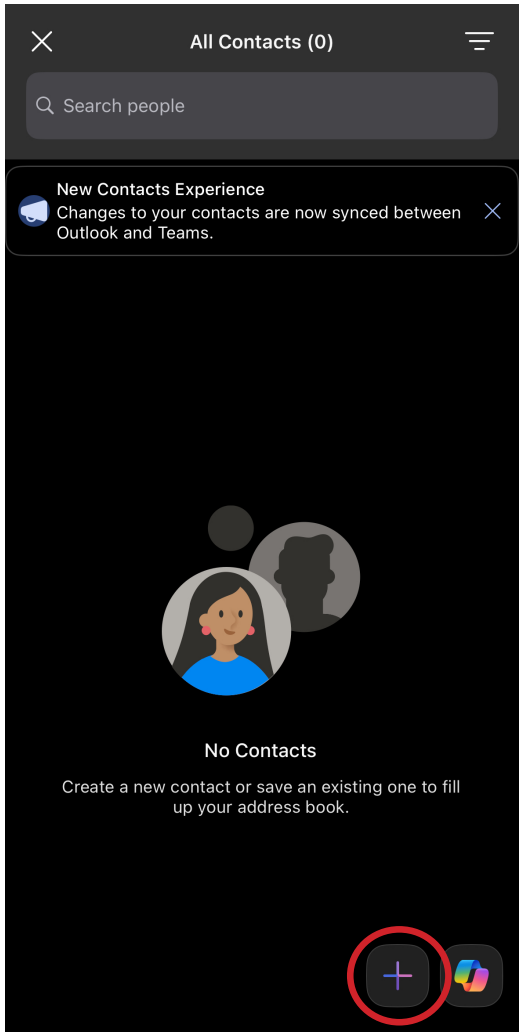
You must not collect, save, or store customer data directly on any personal device, including, but not limited to, phone, tablet, USB, or computer/laptop. This prohibits you from saving contacts to your phone's address book, taking photos of customer information with your personal mobile/tablet devices (i.e. customer licence), requesting customers share information via an unauthorised communication app (e.g., *Whatsapp*), or storing documents in personal cloud storage (e.g., *iCloud, Google Drive*).

These practices apply to **all Suttons employees**, regardless of role, department, location, or employment classification and must be adhered to at all times.

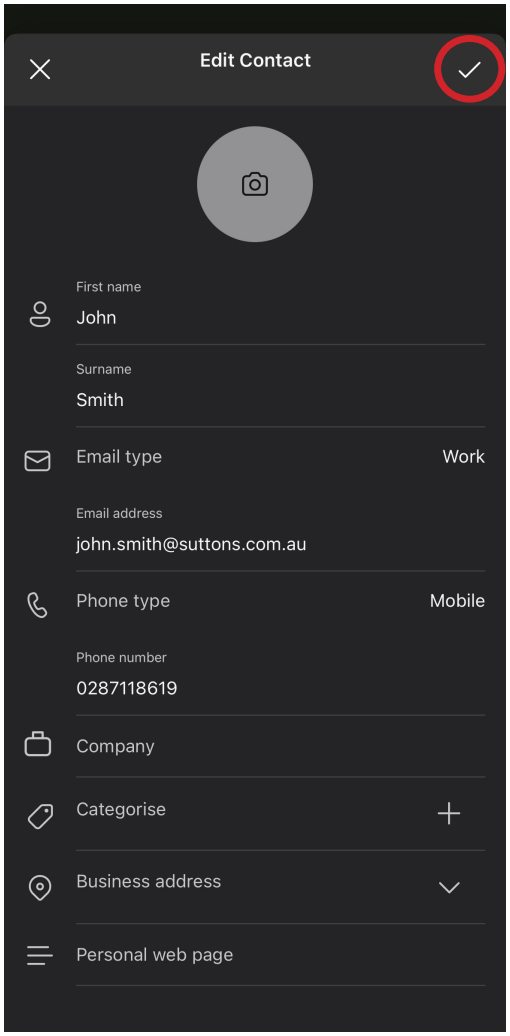
STORING CUSTOMER DETAILS IN THE OUTLOOK APP:



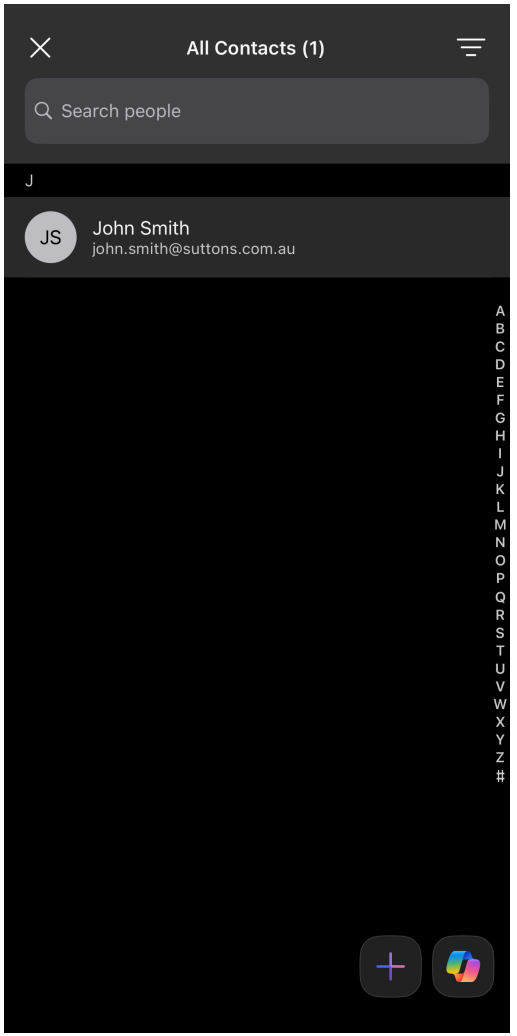
1. Select the Apps icon on the bottom right hand corner. Then select Contacts.



2. Select the PLUS (+) Button



3. Edit contact by typing relevant details in required fields. Press the TICK (✓) icon to save.



4. Customer contact will appear in directory, similar to your phone's internal address book.

IN-DEALER PRIVACY AUDIT CHECKLIST FOR MANAGERS

FOCUS The Collection of Customer Personal Information Using Only Suttons Authorised Systems At All Times

PURPOSE To help managers quickly check that customer data is being collected correctly, securely, and in line with Suttons' Privacy Policy.

1. SYSTEMS AND TOOLS

- ☐ All customer personal information **must only** be collected and stored in Suttons-approved systems. (e.g. Suttons-issued *Outlook* mobile app, *CRM*, *DMS*, and test drive apps such as *Drive Expert*)
- ☐ Customer information is prohibited from being collected or stored outside of Suttons approved apps on any personal devices, including, but not limited to, mobile phones, tablets, USBs, or laptops.
- ☐ Personal email/communication accounts are strictly prohibited from being used to receive, store, or transmit any customer information.

2. COLLECTION PRACTICES

- ☐ Staff must only collect customer information that is necessary to complete the specific transaction or deliver the required service.
- ☐ Staff must clearly explain the purpose for collecting customer information.
- ☐ Storing customer information on personal devices outside Suttons authorised systems is strictly prohibited.
- ☐ Customer information is restricted to Suttons authorised systems only, such as Suttons-issued *Outlook* and approved CRM platforms.
- ☐ Staff must not request customer information that is not required for the specific transaction or service.
- ☐ Customer information is not to be recorded on non-secure materials (e.g., sticky notes, loose paper, notebooks) at any time.

3. USE OF PERSONAL DEVICES (HIGH-RISK CHECK)

- ☐ Photographing customer licences, documents, or system screens on personal mobile/tablet devices is strictly prohibited.
- ☐ Staff are prohibited from saving any customer information in personal contacts or Notes apps on their devices.
- ☐ Collecting customer information through messaging apps (e.g. *WhatsApp*) or any unauthorised communication app is strictly prohibited.

4. ACCESS & AWARENESS

- ☐ Staff understand which systems are Suttons authorised for the collection and handling of customer data.
- ☐ New employees must complete required privacy training before handling or collecting customer information.
- ☐ Records of completed privacy training are current and accurately maintained.

5. RED FLAGS TO ACT ON IMMEDIATELY

- ☐ Staff saying it is "easier" to use personal devices outside authorised systems.
- ☐ Customer information being stored outside Suttons authorised systems.
- ☐ Staff are unsure where or how customer data should be collected and stored.

ESCALATE IMMEDIATELY
if any red flag is identified

Manager
↓
General Manager
↓
Financial Controller
↓
Privacy Officer

Manager Name: _____ Signature: _____

Team Member Name: _____ Signature: _____

☐ I have completed this privacy audit and addressed any issues identified.

Location: _____ Department: _____ Audit Date: _____

Correct use of authorised systems protects our customers, Suttons, and our people.