Suttons

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.

CURRENT VERSION: v1.0 01/26