Acceptable Use Policy Template for Dealership Employees

> **How to use it.** Replace everything in [brackets] with your store's own details, and change any rule that doesn't fit. Fill it in with your general manager, your controller and whoever runs IT. **This template is not legal advice, so have your attorney read your version before anyone signs it.** Ask your attorney about monitoring notice in each state where you have a store (section 8), about the wording in section 10, and about paying staff back for work use of a personal phone and for time spent on it after hours.

Dealership name _____ Effective date _____

1 Who this covers

1.1 This policy covers everyone who works at [Dealership Name], including part-time staff, temps and contractors, on any device used for dealership work.

1.2 We hold customers' personal and financial information. These rules protect them, the store and you.

1.3 The policy owner is [name, title]. If you aren't sure about something, ask [name, phone] before you do it.

2 Company devices and personal phones

2.1 Company computers, tablets and phones are for dealership work. Personal use is [allowed on breaks / not allowed].

2.2 Lock your screen whenever you walk away from it, even for a minute.

2.3 Personal phones and laptops may be used for work only for [approved apps], and only with a screen lock turned on.

2.4 Never save customer information on a personal device. That includes photos, texts and downloads.

2.5 If a device with dealership email or apps on it is lost or stolen, call [name, phone] right away.

2.6 When you leave, you return company devices, and dealership apps and data come off your personal ones.

3 Email and Microsoft 365

3.1 Use your work email for dealership business. Don't forward work email to a personal account.

3.2 Keep dealership files in [OneDrive, SharePoint or the DMS], not in a personal cloud account.

3.3 Send customer information outside the store only through [approved secure method].

3.4 If a message asks you to change bank details, buy gift cards or sign in to see a file, check with the sender at a number you already have.

4 Passwords and multi-factor sign-in

4.1 Use a long password you don't use anywhere else.

4.2 Your login is yours. Don't share it, not even with a manager at month-end.

4.3 Use multi-factor sign-in on every system that asks for it.

4.4 Approve a sign-in prompt only if you just started that sign-in. If you didn't, deny it and report it.

4.5 Never give your password or sign-in code to anyone, even someone who says they're from IT. If someone asks for either, hang up and call [name, phone].

5 Customer information

5.1 Customer information includes driver's licenses, Social Security numbers, credit applications, deal jackets, bank and card details, and [anything else your store adds].

5.2 Open it only when your job calls for it. Looking up a neighbor, an ex or a coworker's deal isn't allowed.

5.3 Keep it where the table below says it belongs. If a customer sends it to you some other way, tell [name] and don't pass it along.

5.4 Deal jackets and credit applications stay in [locked place] when you aren't working on them.

5.5 Paper with customer information goes in [shred bin], never the trash.

Where customer information may and may not go

The information	Where it may go	Where it may not go
Driver's license copy	The DMS or [approved deal system], or the paper deal jacket.	A photo on a personal phone, a text message or personal email.
Credit application	The lender portal or [approved credit system], or the locked deal file.	Regular email, a shared desk folder or an AI tool.
Deal jacket	[Locked file room] or [approved scanning system].	Left out on a desk overnight, or taken home.
Social Security, bank and card numbers	Only the fields built for them in the DMS or [payment system].	Sticky notes, spreadsheets, or anything typed into a chat.
Customer list from the CRM or DMS	[Approved shared location], with [manager]'s approval.	A USB drive, a personal cloud account or a personal phone.
Repair history tied to a name or VIN	The DMS or [approved service system].	A public AI tool or a personal AI account.
Employee and payroll files	[HR system] or the locked HR file, for the people who handle them.	Shared drives, group texts or a manager's personal email.

6 Wi-Fi, USB drives and remote access

6.1 Company devices use [staff Wi-Fi name]. Customers and personal devices use [guest Wi-Fi name].

6.2 Don't plug in a USB drive you found or were handed. Customer information never goes on one.

6.3 Work from outside the building only through [approved remote access], with multi-factor sign-in.

6.4 On public Wi-Fi, [use the VPN / use your phone's hotspot / don't open dealership systems].

6.5 Don't give a caller control of your screen, even one who says they're from IT, until you've checked with [name].

7 Approved software and AI tools

7.1 Use only the software on [where the approved list lives]. To add something, ask [name].

7.2 Don't install apps, browser add-ons, or free or unlicensed software on a company device.

7.3 Keep customer and employee personal information out of AI tools, above all personal AI accounts. Our AI use policy names the approved tools and any exception.

8 Monitoring

8.1 Company email, internet access, phones and devices may be monitored and logged. Don't expect privacy on them.

8.2 The types of monitoring we use are [list them, as your attorney advises].

8.3 [State notice wording from your attorney, if your state requires it.]

9 Reporting a problem

9.1 Tell [name, phone] right away if you clicked something odd, lost a device, saw a strange login or sent customer information to the wrong place.

9.2 Don't try to fix it or delete anything. Make the call first.

9.3 You won't get in trouble for quickly reporting an honest mistake.

10 Signing it

10.1 Breaking these rules can lead to [discipline, up to and including termination].

10.2 Nothing here stops you from talking about pay, hours or working conditions, or from reporting a concern to a government agency.

10.3 We'll go over this policy with you at hire and [how often], and ask you to sign again when it changes.

10.4 I've read this policy and had the chance to ask questions.

Printed name _____ Signature _____ Date _____

Finished the policy?
A complimentary IT and cybersecurity assessment reviews the technology behind your policy, including AI tool use in personal accounts, and puts the findings in a written report.

heliontechnologies.com/it-assessment/

Acceptable use policy template from Helion Technologies. A starting point, not legal advice; the final policy is the dealership's own. © 2026 Helion Technologies.