security · privacy · plan-tier decisions for small business

FREE OR PAID
THE SMART CHOICE

Picking the Right AI Tool — what actually protects your business data, and what just changes the price.

DIAMOND BUSINESS COMMUNICATIONS

UPDATED OCTOBER 2026

A MANAGED SERVICE PROVIDER

what we cover today

THE AGENDA

01	The AI market: personal, business, and enterprise
02	Live demo: same task, different account types
03	What happens to your data after you type
04	How model training differs from encryption and governance
05	Five questions before any AI gets company information
06	Choose a business-base tool and protection level

DIAMOND AI

you leave today with

THREE DECISIONS

A BUSINESS-BASE TOOL

ChatGPT, Claude, Gemini, or Copilot — chosen around the workflow your team will actually use.

A DATA-HANDLING RULE

Know whether the account is consumer or organizational, whether training is allowed, and what controls apply.

A VENDOR CHECKLIST

Ask about training, encryption, contracts, retention, access controls, audit, DLP, and compliance.

THE AI TOOL MARKET: 3 LEVELS TO KNOW

Think account type and governance, not just price.

LIVE DEMO: SAME TASK, DIFFERENT ACCOUNTS

The output may look similar. The data terms can be very different.

three levels every small business should know

CONSUMER → BUSINESS → ENTERPRISE

PERSONAL

PERSONAL / CONSUMER

Free or paid. Useful for individual productivity. Data-use choices vary by vendor and settings. Paid does not automatically mean business-protected.

BUSINESS

BUSINESS / TEAM

Commercial terms. Across the vendors reviewed, business content is generally excluded from model training by default. Encryption and organizational controls are present, but features vary.

ENTERPRISE

ENTERPRISE

Adds deeper administration, governance, retention, audit, identity, compliance, residency, and/or key-management options depending on vendor.

stop using price as

THE SECURITY SHORTCUT

“Not using your data to train the AI does NOT mean your data is fully protected or governed.”

A $20 CONSUMER SUBSCRIPTION

May improve capability without changing the legal or administrative framework.

A WORK ACCOUNT

May provide business protections at a very different price point.

Ask yourself: what account type am I using, and what terms protect the data?

a better core privacy principle

THE ONE RULE TO REMEMBER

“Consumer AI can be useful, but do not assume free means training or paid means protected.”

Before entering confidential business information, verify:

- ACCOUNT TYPE
- TRAINING POLICY
- CONTRACTUAL TERMS
- ENCRYPTION
- RETENTION
- ACCESS CONTROLS

ONE TASK, THREE ACCOUNTS

Task: draft a follow-up email to a client who missed a meeting

A **Personal / consumer account**
Free tier, everyday sign-in

B **Paid personal / consumer account**
The $20-style subscription

C **Business / work account**
Organizational, commercial terms

Score: output usefulness + data-handling posture + admin/governance

WHAT TO WATCH FOR

OUTPUT EXPERIENCE

- Quality and specificity
- Usage limits and speed
- Fit with your workflow
- Need for re-prompting
- Integration with business apps

DATA & GOVERNANCE SIGNALS

- Consumer vs. commercial terms
- Is model training allowed?
- Encryption statements
- Admin / identity controls
- Retention, audit and DLP
- Compliance options

WHAT THE DEMO SHOULD SHOW

- ✓ Free and paid consumer plans are still consumer environments
- ✓ Model-training rules differ by vendor and can depend on user settings
- ✓ Business/Team offerings generally exclude business data from training by default
- ✓ Encryption is not an Enterprise-only feature
- ✓ Enterprise usually adds deeper governance, identity, auditing, retention, residency, key management, and compliance options

WHAT HAPPENS TO YOUR DATA: AFTER YOU TYPE

Training, encryption, retention, and governance are different questions.

ASK THE RIGHT QUESTIONS

1

TRAINING

Will the provider use prompts or outputs to improve models? Is that default, opt-in, opt-out, or contractually excluded?

2

PROTECTION

Is data encrypted in transit and at rest? What identity, permissions, tenant isolation, and admin controls apply?

3

GOVERNANCE

Can admins control retention and audit activity? Are there controls for data loss, compliance, residency, or encryption keys?

These are separate axes — “not used for training” does not mean “zero retention,” and “encrypted” does not mean “appropriate for every regulated workload.”

risk by data type

WHAT TO PROTECT

TREAT AS SENSITIVE

- Client + financial information
- HR, salary or personnel records
- Customer PII such as SSN
- Legal documents and contracts
- Proprietary pricing or processes
- Regulated health or financial data

LOWER-RISK EXAMPLES

- Public marketing copy
- Generic templates with no client names
- Brainstorming with synthetic examples
- Public industry research
- Drafts based only on public information

Sensitive data should go only into an organizationally approved AI service configured for that data class.

updated framework

THE DATA-SAFETY THRESHOLD

TRAINING POLICY | COMMERCIAL TERMS | ENCRYPTION | IDENTITY | RETENTION | AUDIT / DLP | COMPLIA

+

Use an approved organizational account with documented protections that match the data.

This replaces “the paid tier that actually protects you.” Protection is a stack of controls, not one price point.

the three tiers side by side

CONSUMER VS BUSINESS VS ENTERPRISE

CONSUMER

Personal terms; training use varies by vendor/settings; security safeguards exist; limited organizational administration.

BUSINESS / TEAM

Commercial terms; business content generally not used for model training by default; encryption and admin/workspace controls vary by provider.

ENTERPRISE

Adds advanced governance/security options: enhanced SSO/SCIM, audit/compliance APIs, custom retention, data residency or customer-managed keys.

follow the money

WHAT YOU'RE ACTUALLY PAYING FOR

CONSUMER PAID	More usage, features, models or priority — while remaining under consumer terms.
BUSINESS / TEAM	Organizational workspace + commercial data-handling commitments + administration.
ENTERPRISE	Deeper governance, compliance and security options.

Do not use a universal dollar threshold — vendor packaging and included protections differ.

WHERE THE PROTECTION CHANGES

Platform	Personal / Consumer	Business / Work	Enterprise
ChatGPT	Free / Plus / Pro: consumer controls; training may occur unless user opts out	Business: training excluded by default; encrypted at rest/in transit	Enterprise: adds advanced access, retention and enterprise controls
Copilot	Personal account: consumer terms and privacy controls	Copilot Chat + eligible work account: EDP; no foundation-model training	Paid Microsoft Copilot: EDP + broader org grounding; controls depend on M365 plan
Claude	Free / Pro / Max: user chooses model-improvement setting	Team / Claude for Work: commercial terms; no training by default	Enterprise: adds audit logs, SCIM, retention, Compliance API, CMEK
Gemini	Personal Gemini: consumer privacy/activity settings apply	Qualifying Workspace: enterprise-grade protections; no training outside domain without permission	Gemini Enterprise: adds IAM, audit, data residency, VPC controls, CMEK

the gap most people miss

CONSUMER VS COMMERCIAL

PAID CONSUMER

- Better capabilities may come with the subscription
- Still governed as an individual/consumer service
- Training preference may remain user-controlled
- Not the same as organizational administration or commercial terms

BUSINESS / WORK

- Commercial or enterprise terms apply
- Business content generally excluded from model training by default
- Organizational security/admin controls
- Governance depth varies by vendor and license

The material difference is the legal and administrative context — not the monthly price.

WHERE TO VERIFY DATA SETTINGS

CHATGPT – PERSONAL

Settings → Data Controls → "Improve the model for everyone" → OFF

OpenAI says personal Free, Plus and Pro users can turn training off. New conversations will not be used to train OpenAI's models.

CLAUDE – PERSONAL

Settings → Privacy → "Help Improve our AI models" → OFF

Incognito chats are not used to improve Claude. New chats and coding sessions will not be used for future model training, subject to Anthropic's stated safety exceptions.

Microsoft & Google: demonstrate sign-in context and the managed Workspace/M365 admin controls instead of a personal training toggle.

BEFORE ANY AI GETS YOUR DATA: THE 5 QUESTIONS

Five questions to answer before company information goes in.

KNOWING WHEN CONSUMER AI: STOPS BEING ENOUGH

The honest guide to choosing the right account type.

your action plan

PICKING YOUR AI MODEL

Then pick the right account type for the data.

THE EXERCISE ↓

five clear signs

YOU NEED AN ORGANIZATIONAL AI PLAN

1. Employees routinely use AI for real client or company work
2. Confidential, personal, financial, HR, legal, or regulated data is involved
3. You need centralized identity, access, offboarding, or policy enforcement
4. You need audit, retention, DLP, eDiscovery, residency, or compliance controls
5. A client, insurer, auditor, board, or regulator asks how AI data is governed

CONSUMER OR BUSINESS?

CONSUMER CAN FIT WHEN

- You are exploring with public or synthetic data
- No client/confidential/regulated data is used
- AI is individually managed and policy permits it
- You understand and configure the privacy controls

MOVE TO BUSINESS / WORK WHEN

- Real business data enters prompts or files
- Multiple staff need consistent governance
- You need commercial data terms
- You need centralized identity/admin controls
- Audit, retention, DLP, or compliance matters

Even with a business tier, use an approved-data policy — the license alone doesn't make every data type appropriate.

the value question

DOES THE BUSINESS TIER PAY FOR ITSELF?

Security value is not just speed.

GOVERNANCE

Centralize who can use AI and under what account.

RISK REDUCTION

Separate approved business use from unmanaged consumer use.

OPERATIONAL FIT

Add organizational grounding, admin features, and workflow integration where supported.

exercise

MAKE YOUR DECISION NOW

1. Name the AI task that would help you most
2. Identify the data involved: public, internal, confidential, personal, or regulated
3. Check whether your current account is personal or organizational
4. Verify training, contract, encryption, retention, access, audit/DLP, and compliance controls
5. Approve one home-base tool and document what data employees may use

which tool

SHOULD YOU CHOOSE?

CHATGPT OR CLAUDE

Strong general-purpose choices when you want a dedicated AI workspace. For business use, choose the commercial workspace when company data is involved.

GEMINI OR COPILOT

Strong fit when your organization already lives in Google Workspace or Microsoft 365 and wants AI governed inside that ecosystem.

Conversation starter: How many platforms does it take to produce your work? What does that cost per person — and what is the ROI and the security worth to you?

before you go

THREE THINGS TO REMEMBER

1 · PRICE IS NOT THE SECURITY MODEL

Free versus paid is too simple. Personal versus organizational account type is the better first question.

2 · NO TRAINING ≠ FULL GOVERNANCE

Encryption, retention, identity, audit, DLP, residency, contracts and compliance all matter too.

3 · USE ONE APPROVED HOME BASE

Standardize the tool, account type, permitted data, and governance rules for your team.

“Choose AI based on the data and controls, not just the monthly price.”

verified resources

GO TO THE SOURCE

OpenAI	Business data privacy, security and compliance	openai.com/business-data
Microsoft	Enterprise Data Protection in Copilot and Copilot Chat	learn.microsoft.com
Anthropic	Commercial model-training policy + Enterprise plan controls	privacy.claude.com
Google Workspace	Generative AI privacy/security hub	knowledge.workspace.google.com
Google Cloud	Gemini Enterprise security overview	docs.cloud.google.com

Use vendor documentation — not social posts — as the source of truth, because plans and policies change.

questions? let's talk.

WE'RE HERE TO HELP

Helping New Jersey SMBs and nonprofits adopt AI with security, governance, and business value in mind.

WWW.DIAMONDBC.NET

609-642-9300

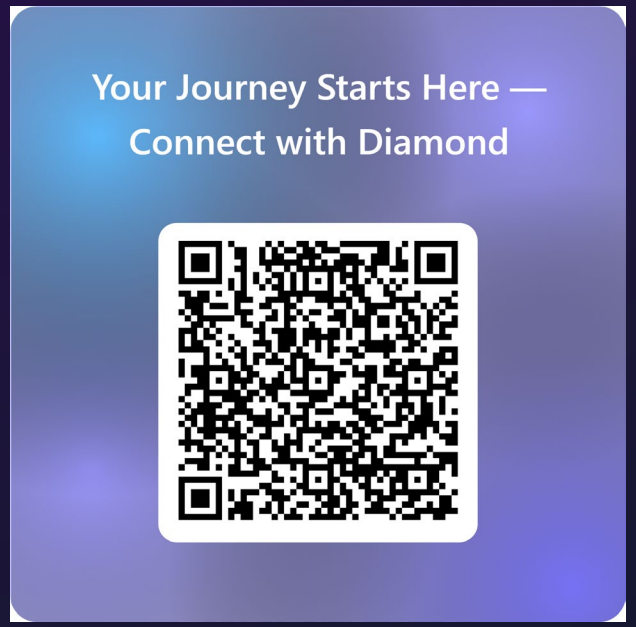
DIAMOND AI

THANK YOU

Use AI boldly. Govern the data deliberately.

DIAMOND
BUSINESS COMMUNICATIONS

LET US HELP YOU SUCCEED!



Use AI boldly. Govern the data deliberately.

DIAMOND AI