Session 2 Handout: Protecting People's Information

FAST-17 Responsible AI for All Staff · 7formations · Instructor: Wadood Chaudhary · All examples fictional · Not legal advice · Suggested reading: Svekis, AI Literacy for All Employees (2026), chapter 10

Why this session matters

The most common AI mistake at work is not a bad answer. It is pasting the wrong thing into the wrong tool. In Pew Research Center's February 2026 survey, about seven in ten Americans said they expect AI to make their personal information less secure. Everyday choices by employees decide whether that happens.

Key concepts

1. Three kinds of sensitive information

Kind	Examples
Personal	Names with contact details, employee records, customer complaints
Confidential business	Pricing, bids, client lists, unreleased financials, drawings
Regulated	Name + SSN, license or state ID, or account or card number (G.L. c. 93H); health information; tax information

Massachusetts **201 CMR 17.00** requires businesses that hold residents' personal information to keep a written security program. Where data goes, including into AI tools, is part of it.

2. What AI tools store, remember, and train on

- The chat itself is usually stored by the vendor for some period.
- **Memory** features can carry details across chats unless turned off.
- **Training:** business plans generally do not use your data to train models by default; consumer settings may. Check your tool's help pages and your employer's policy.

3. Safe data practices

Approved tools with work accounts only · Share only what the task needs (minimization) · Replace identifiers with placeholders such as [CLIENT NAME] · Never route around policy with a personal account or a coworker's login · Report slips the same day.

4. AI-enabled scams

The FBI has warned (December 2024, and again in 2026) that criminals use AI-generated voice, video, and text to impersonate people victims trust. Red flags: urgency, secrecy, new payment details, requests for data or credentials. The fix: **verify through a known number or channel**, never the one in the message, and report it.

Worked example

A Back Bay Accounting Partners (fictional) accountant pastes a client's name, SSN, income, and bank account into a free chatbot to polish an email. Two mistakes: the wrong tool and unnecessary data. The data-safe version uses the approved tool and placeholders: "Rewrite this client email in a warm, plain tone. The refund amount is [AMOUNT]. Ask the client to confirm deposit details through the secure portal." If the slip already happened: report it the same day so the firm can assess it.

Try this before session 3

- Find your approved tool's memory and data settings.
- Read Svekis chapter 10.