

How to Use AI Safely And Responsibly

June 26, 2026

A Digital Safety Guide

Prepared for Pennswood Residents by the

Safety Advisory Committee

And

The AI Users Group

Guide: How to Use AI Safely and Responsibly

A practical safety guide for residents using AI tools like Copilot, ChatGPT, and Gemini.

1. Start With the Right Mindset

AI is a helpful assistant — not an authority, not a doctor, not a lawyer, and not a replacement for human judgment.

Residents should think of AI as:

A smart helper that can draft, explain, summarize, and suggest — but still needs supervision.

2. Protect Your Personal Information

AI tools are safe to use, but residents should avoid sharing sensitive details unless they fully understand the context.

Do NOT enter:

- Social Security numbers
- Bank account or credit card numbers
- Passwords or PINs
- Medical record numbers
- Private family disputes
- Anything you wouldn't want written on a postcard

Safe to enter:

- General questions
 - Public information
 - Drafts of letters
 - Summaries of articles
 - Creative writing
 - Everyday tasks
-

3. Be Cautious With Health, Legal, and Financial Topics

AI can explain concepts clearly, but it cannot replace professionals.

Use AI for:

- Understanding terms (“What is a living will?”)
- Preparing questions for your doctor or lawyer
- Summaries of public information
- Drafting notes or letters

Do NOT rely on AI for:

- Diagnosing symptoms
- Making legal decisions
- Financial planning
- Emergency situations

Always confirm important information with a qualified professional.

4. Verify Important Information

AI can make mistakes — confidently.

Residents should double-check anything that affects their safety, money, or well-being.

Simple ways to verify:

- Ask the AI to check its own work
 - Request sources
 - Compare with trusted websites
 - Ask follow-up questions
 - Consult a human expert when needed
-

5. Recognize Scams and Misinformation

AI can help residents stay safer online, but they should be aware of risks.

AI will NOT:

- Ask for money
- Ask for passwords
- Call you on the phone
- Demand urgent action

If something feels suspicious:

- Stop
 - Ask the AI to analyze it
 - Check with a trusted person
 - Report scams to community staff if appropriate
-

6. Use Image Generation Responsibly

AI can create images, but residents should understand the boundaries.

Allowed:

- Creative artwork
- Illustrations
- Decorative borders
- Imaginary scenes

Not allowed:

- Images of real political candidates
 - Trademarked characters
 - Harmful or misleading images
 - Deepfakes of real people
-

7. Understand AI Memory and Privacy Settings

Some AI tools can remember preferences (if enabled).

Residents should know:

- Memory can be turned on or off
- They control what is remembered
- They can ask the AI to forget something
- They can delete past conversations

This gives residents confidence and control.

8. Keep a Healthy Skepticism

AI is helpful, but not perfect.

Residents should remember:

- AI can be wrong
- AI can sound confident even when incorrect
- AI does not “know” things — it predicts
- AI is a tool, not a decision-maker

9. Use AI to Enhance — Not Replace — Human Connection

AI can help residents:

- Write emails
- Prepare speeches
- Summarize articles
- Learn new skills
- Stay organized

But it should never replace:

- Family conversations
- Medical advice
- Legal counsel
- Personal judgment
- Community relationships

10. Summary Box

Use AI safely by:

- Protecting personal information
 - Verifying important facts
 - Avoiding sensitive financial/medical/legal decisions
 - Watching for scams
 - Using image generation responsibly
 - Managing memory and privacy settings
 - Keeping a balanced, thoughtful approach
-

Twenty Cautionary Notes For Using AI Safely

AI is useful, but it should be treated like a very capable assistant, sometimes needing human judgment and fact checking.

1. **Do not put private, confidential, or sensitive information into an AI dialog.** Once disclosed, it cannot truly be clawed back. Even if a system says it protects your data, you may not know how the information is stored, reviewed, retained, or used.
2. **Do not grant AI broad access to other apps, websites, files, calendars, email, financial accounts, password managers, or medical portals unless you fully understand the risk.** Convenience can quietly become overexposure. The more access you grant, the more damage a mistake, breach, or misuse could cause.
3. **Assume AI may use prior conversations, memories, uploaded files, or connected data as context for later answers.** This can be helpful, but it can also bias the response, reinforce your assumptions, or create a false sense that the AI “knows” more than it really does.
4. **Recognize that AI is often designed to be agreeable.** It may flatter, affirm, or smooth over disagreement. Ask directly for candor, weaknesses, contrary evidence, and alternative interpretations.
5. **Do not mistake fluency for truth.** AI writes well, but polished language can conceal uncertainty, weak sourcing, missing context, or outright error.
6. **Watch for overconfidence.** AI often sounds more certain than the available information justifies. This is especially risky in legal, medical, financial, political, technical, or organizational matters.
7. **Verify important facts independently.** Names, dates, quotes, statistics, laws, policies, prices, contact information, and current events should be checked against reliable sources before use.
8. **Do not rely on AI as a final authority.** Treat it as a drafting assistant, research aide, brainstorming partner, or tutor — not as a judge, lawyer, doctor, accountant, security expert, or fiduciary.
9. **Be cautious with AI-generated citations.** It may cite sources inaccurately, misunderstand them, or appear to support a claim that the source does not actually support.
10. **Beware of hidden assumptions.** AI may fill gaps with plausible guesses. It may not clearly distinguish between what it knows, what it infers, and what it is merely assuming.

11. **Understand that AI can mirror your framing.** If your question contains a mistaken premise, AI may build on that premise instead of challenging it unless you ask it to do so.
12. **Do not let AI replace human judgment in matters involving people.** It can help draft language or analyze options, but it cannot understand relationships, motives, dignity, grief, trust, fear, loyalty, or moral responsibility the way humans must.
13. **Be careful using AI to summarize long documents.** It may miss qualifications, exceptions, footnotes, tone, or context. For contracts, policies, legal notices, medical records, and financial statements, the details matter.
14. **Be alert to privacy risks in uploads.** A document may contain metadata, names, addresses, financial details, hidden comments, tracked changes, or other information you did not intend to share.
15. **Do not assume AI-generated text is original or appropriate for publication without review.** It may echo common phrasing, reproduce familiar structures, or create text that sounds generic, artificial, or unlike your authentic voice.
16. **Remember that AI has a recognizable style.** It often favors balance, smooth transitions, lists of three, moral symmetry, and confident closure. Good editing is needed to make the result sound human, specific, and truly yours.
17. **Be especially cautious when AI gives instructions for computers, security, finance, health, law, or physical safety.** A small error in these areas can have serious consequences.
18. **Do not use AI to make decisions about other people without transparency and accountability.** This includes hiring, discipline, caregiving, resident relations, eligibility, benefits, or complaints. AI may reflect bias in its training data or in the information supplied to it.
19. **Be aware that AI can be manipulated.** Malicious prompts hidden in emails, documents, or web pages can try to influence what an AI system does, especially if it has access to tools or connected accounts.
20. **Keep responsibility where it belongs.** AI can assist, but the human user remains responsible for what is shared, sent, published, decided, or done.
