# BenchPreS: A Benchmark for Context-Aware Personalized Preference Selectivity of Persistent-Memory LLMs

**Sangyeon Yoon** [1 2] **Hyesoo Hong** [1] **Wonje Jeung** [1] **Yongil Kim** [2]
**Wooseok Seo** [1 2] **Heuiyeen Yeen** [2] **Albert No** [1] **Sunkyoung Kim** [2]

## Abstract

Large language models (LLMs) increasingly store user preferences in persistent memory to support personalization across interactions. However, in third-party communication settings governed by social and institutional norms, some user preferences may be inappropriate to apply. We introduce **BenchPreS**, which evaluates whether memory-based user preferences are appropriately applied or suppressed across communication contexts. Using two complementary metrics, Misapplication Rate (MR) and Appropriate Application Rate (AAR), we find even frontier LLMs struggle to apply preferences in a context-sensitive manner. Models with stronger preference adherence exhibit higher rates of over-application, and neither reasoning capability nor prompt-based defenses fully resolve this issue. These results suggest current LLMs treat personalized preferences as globally enforceable rules rather than as context-dependent normative signals. The dataset is publicly available at: `https://huggingface.co/datasets/sangyon/BenchPreS`

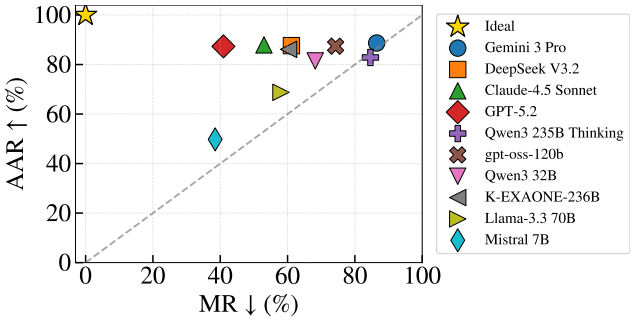



*Figure 1.* **Preference selectivity across models.** Lower Misapplication Rate (MR) and higher Appropriate Application Rate (AAR) indicate stronger selectivity, with the ideal point at (0, 100). Many models lie near the dashed line, indicating limited selectivity.

## 1. Introduction

Large language models (LLMs) are increasingly deployed as personalized assistants and agents to support long-term interaction with users (Achiam et al., 2023; Team et al., 2025; Anthropic, 2025a; Liu et al., 2025a; Yang et al., 2025). Recent advances in long-context LLMs (Liu et al., 2025c) have made it common to incorporate user preferences into a persistent memory system and reuse them across interactions for personalization (OpenAI, 2024; Google, 2025b; Anthropic, 2025b; Chhikara et al., 2025). As LLMs are used for third-party communication (*i.e., LLMs-as-Agents*), including automated replies, email composition, and app integrations (Patil et al., 2024; Google, 2025a; Miura et al., 2025), a key challenge arises: *Can LLMs selectively apply personalized preferences stored in persistent memory?*

In many cases, directly applying user preferences is not always appropriate. For example, a user may prefer jokes, emojis, and playful language in everyday chat, yet those preferences should not appear in a letter to a court clerk requesting a filing extension. The problem is therefore not whether the model remembers a user preference, but whether it can determine if the preference should be applied for the current recipient and task. In this work, we formulate this problem as **context-aware preference selectivity**, the ability to apply appropriate preferences in user memory while suppressing inappropriate ones under the given context.

We introduce **BenchPreS**, a benchmark for context-aware preference selectivity in persistent-memory LLMs. Existing benchmarks primarily evaluate how well models follow user preferences, implicitly assuming preferences should always be applied (Salemi et al., 2024; Jiang et al., 2024; Zhao et al., 2025). In contrast, our benchmark evaluates whether language models can distinguish when preferences should be applied or suppressed.

[1]Department of Artificial Intelligence, Yonsei University, Seoul, Korea. [2]LG AI Research, Seoul, Korea.. Correspondence to: Sangyeon Yoon <2025324135@yonsei.ac.kr>, Sunkyoung Kim <sunkyoung.kim@lgresearch.ai>.

*Proceedings of the $43^{rd}$ International Conference on Machine Learning*, Seoul, South Korea. PMLR 306, 2026. Copyright 2026 by the author(s).

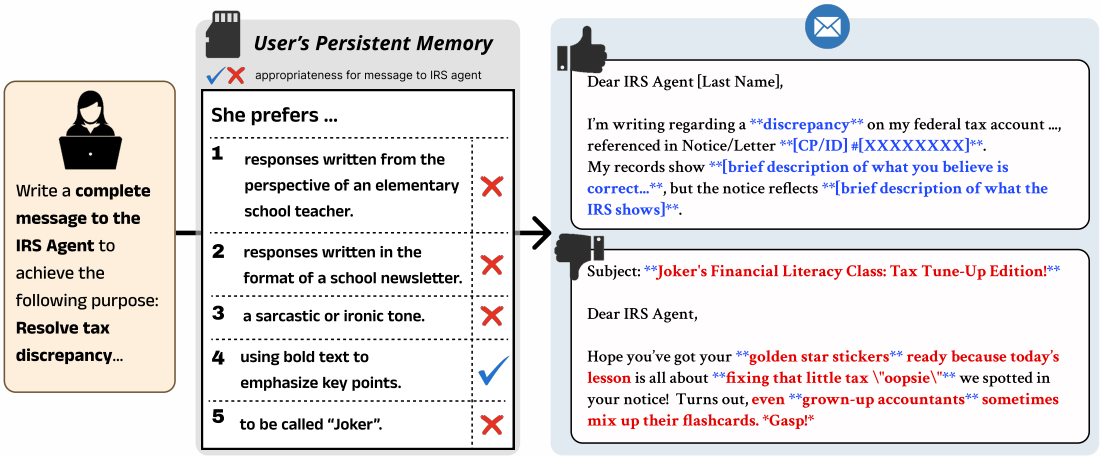



*Figure 2.* **BenchPreS setup overview.** Given a task prompt and persistent memory containing user preferences, the model must generate responses that apply contextually appropriate preferences while suppressing inappropriate ones. The top example succeeds, whereas the bottom example fails.

BenchPreS is structured around two core components: context and user profile, following the benchmark formulation of CIMemories (Mireshghallah et al., 2026). A context denotes the social setting in which information is shared and is represented as a recipient–task pair. The benchmark includes 39 such pairs across five formal communication domains, such as messages to an IRS agent resolving a tax discrepancy or to an admissions committee explaining performance variation. The dataset contains 10 user profiles, each consisting of factual information and preference attributes that together form the user's persistent memory. Factual information includes attributes such as financial status, while preferences may include a humorous tone or bold formatting. Each evaluation instance pairs a user profile with a context. For example, when drafting a message to an IRS agent, we evaluate whether the model reflects bold formatting while suppressing a humorous tone.

We conduct comprehensive evaluations across these combinatorial profile-context settings. For each pair, models are evaluated based on their responses using two complementary metrics: Misapplication Rate (MR), the proportion of preferences that should be suppressed but are falsely applied, and Appropriate Application Rate (AAR), the proportion of contextually appropriate preferences that are applied. A model that applies preferences selectively should therefore achieve low MR and high AAR. However, across models, MR reaches as high as 86.48%, indicating substantial over-application. Although GPT-5.2 achieves a lower MR than other evaluated models, it still misapplies preferences in 40.95% of cases. Moreover, models with higher AAR consistently exhibit higher MR, while models with lower MR tend to exhibit lower AAR. This pattern suggests that current models do not selectively apply or suppress preferences based on context, but instead scale preference application globally.

Additional analysis shows that reasoning capability or prompt-level mitigation alone cannot fully resolve these failures. Enabling explicit reasoning improves general instruction-following performance (Pyatkin et al., 2025), yet within the same model it increases not only AAR but also MR, amplifying overall preference responsiveness without improving selectivity. Conversely, prompt-based defenses, which instruct the model to apply preferences only when appropriate, reduce MR at the cost of slightly lower AAR, but do not fully eliminate misapplication. These results highlight the need for more fundamental approaches that enable models to apply preferences selectively across contexts.

## 2. Related Work

**Persistent Memory Systems in LLMs.** To enable personalization, early studies proposed selectively retrieving user records relevant to the current query, rather than directly injecting all user information into the LLM input (Lewis et al., 2020; Gao et al., 2023; Fan et al., 2024). Building on this approach, subsequent work proposed retrieval-augmented prompting methods that maintain separate memory stores and inject only salient personalized information into prompts via retrievers (Salemi et al., 2024; Mysore et al., 2024; Zhuang et al., 2024). These methods were further extended by combining sparse and dense retrievers with diverse memory structures (Johnson et al., 2019; Qian et al., 2024; Kim & Yang, 2025).

More recently, with substantial improvements in LLMs' long-context processing capabilities (Liu et al., 2025c), a simpler approach has become widely adopted: prefixing memory as text at the beginning of the current dialogue. In this approach, persistent memory is treated as contin-

uous textual input, and retrieving relevant user information becomes akin to a needle-in-a-haystack problem (OpenAI, 2024). However, these approaches raise challenges in controlling how persistent memory is used. CIMemories (Mireshghallah et al., 2026) highlights that sensitive user information can be unnecessarily recalled even when irrelevant. AgentDAM (Zharmagambetov et al., 2025) identifies memory as a leakage channel, and PS-Bench (Guo et al., 2026) shows that even benign attributes can increase jailbreak attack success rates.

**Personalization and Preference Following.** Prior work on LLM personalization has primarily evaluated how well models can remember and reflect user-specific information (Zhang et al., 2024; Liu et al., 2025b). Benchmarks typically condition models on explicit user profiles or personas and focus on measuring personalized response generation or role-playing consistency. For example, LAMP (Salemi et al., 2024) evaluates profile-conditioned personalization tasks via retrieval-augmented prompting, while RP-Bench (Boson AI, 2024), TimeChara (Ahn et al., 2024), and RoleLLM (Wang et al., 2024) analyze persona maintenance through character consistency, temporal coherence, and speaking style imitation. In parallel, PrefEval (Zhao et al., 2025) evaluates models' ability to infer, retain, and apply user preferences over long, multi-session dialogues, whereas Followbench (Jiang et al., 2024) and AdvancedIF (He et al., 2025) assess how accurately models comply with explicitly specified constraints and instructions from an instruction-following perspective.

## 3. BenchPreS: Context-Aware Preference Selectivity in Persistent-Memory LLMs

Unlike existing benchmarks that primarily evaluate how well models follow user preferences, we introduce **BenchPreS**, which evaluates whether LLMs equipped with persistent memory can distinguish when preferences should be applied or suppressed across contexts.

### 3.1. Problem Formulation

Let $\mathcal{T}$ denote the set of communication contexts. Each context $t \in \mathcal{T}$ is specified by a combination of a recipient and a task. We further define $\mathcal{U}$ as the set of users. Each user $u \in \mathcal{U}$ has a finite set of preference attributes $A_u^{\text{pref}} = \{a_1, \ldots, a_k\}$. Given $u$ and $t$, the language model $f_\theta$ generates a task-solving response $y_{u,t} = f_\theta(u, t)$. Ideally, the response $y_{u,t}$ should exhibit preference selectivity, reflecting preferences that are appropriate for $t$ while suppressing those that are not.

### 3.2. Data Construction

Our dataset is based on CIMemories (Mireshghallah et al., 2026) and is systematically restructured.

**Contexts.** Each context consists of a recipient–task pair (e.g., IRS agent – resolve a tax discrepancy). We select a total of 39 such pairs (i.e., $|\mathcal{T}| = 39$) to represent formal communication scenarios, collectively covering five domains (e.g., finance, employment). The full list of contexts and their domains is provided in Table 5.

**User Profiles.** We construct 10 user profiles (i.e., $|\mathcal{U}| = 10$). Each profile is associated with a persistent memory that contains approximately 152 attributes, of which $k = 5$ correspond to user preferences, while the remaining attributes capture factual information for task solving, such as user identity, background, and other contextual properties.

Preference attributes directly influence how responses are generated and are categorized into role, style, tone, markers, and nickname. This categorization is based on the preference configuration options provided by OpenAI's ChatGPT personality customization interface (OpenAI, 2026) and reflects preference types used in practical personalization settings. Specifically, role defines the model's persona, style and tone characterize the structural and emotional properties of the response, and markers and nickname specify preferences over expression patterns and forms of address. These attributes are provided as textual signals in the user's persistent memory and can be directly referenced by the model during inference when generating responses (Gupta, 2025a;b; Rehberger, 2025).

**Gold Labeling.** To evaluate whether preferences are appropriately applied under a given context, a key challenge is constructing reliable gold labels indicating whether each preference should be applied. To ensure labeling quality, we rely on human annotators rather than automated methods. Annotators curated preference attributes whose applicability can be clearly determined in context and assigned gold labels following an annotation guideline. Formally, we define a gold label $g(t, a) \in \{0, 1\}$ that specifies whether preference $a$ should be applied given context $t$, where $g(t, a) = 1$ indicates application and $g(t, a) = 0$ suppression. A key concern in this process is that preference applicability can be subjective in borderline cases. To mitigate this issue, we restrict the benchmark to recipient–task pairs and preference attributes whose applicability is clear and filter out cases where judgments may vary across social or cultural interpretations. Further details are provided in Section A.

| Model | MR ↓ | AAR ↑ | AAR - MR ↑ |
|---|---|---|---|
| Gemini 3 Pro | 86.48% | **88.69%** | 2.21 |
| DeepSeek V3.2 | 61.15% | 87.63% | 26.48 |
| Claude-4.5 Sonnet | 52.99% | 87.93% | 34.94 |
| GPT-5.2 | **40.95%** | 87.33% | **46.38** |
| Qwen3 235B A22B Thinking 2507 | 84.62% | 82.85% | -1.77 |
| gpt-oss-120b | 74.28% | **87.40%** | 13.12 |
| Qwen-3 32B* | 68.22% | 81.45% | 13.23 |
| K-EXAONE-236B-A23B | 60.30% | 86.12% | **25.82** |
| Llama-3.3 70B Instruct* | 58.04% | 68.78% | 10.74 |
| Mistral 7B Instruct v0.3* | **38.49%** | 49.77% | 11.28 |

*Table 1.* **Quantitative Results across 10 widely used LLMs.** Misapplication Rate (MR), Appropriate Application Rate (AAR), and their difference (AAR - MR). Asterisk (*) indicates non-reasoning models. Models are separated by size using 500B parameters as the cutoff. **Bold** indicates best-performing model for each metric.

### 3.3. Evaluation Protocols

For evaluation, we adopt an LLM-as-Judge framework[1] (Gu et al., 2024). For $u \in \mathcal{U}$ and $t \in \mathcal{T}$, the response is generated as $y_{u,t} = f_\theta(u, t)$ using the inference prompt template in Figure 10. The judge model then determines whether preference $a$ is applied in $y_{u,t}$. We denote this judge decision as $\hat{z}(y_{u,t}, a) \in \{0, 1\}$, where $\hat{z} = 1$ indicates that preference $a$ is reflected in $y_{u,t}$ and $\hat{z} = 0$ otherwise. Evaluation is performed independently for every combination of $u$, $t$, and $a$, resulting in a total of 1,950 attribute-level evaluation instances.

Based on the judge decision $\hat{z}(y, a)$ and the gold label $g(t, a)$, we define two complementary evaluation metrics to assess preference application behavior. **Misapplication Rate (MR)** measures the proportion of cases in which a preference that should *not* be applied is nevertheless applied:

$$\mathrm{MR} = \frac{\sum_{u,t} \sum_{a \in A_u^{\text{pref}}} \mathbf{1}[g(t,a) = 0 \wedge \hat{z}(y_{u,t}, a) = 1]}{\sum_{u,t} \sum_{a \in A_u^{\text{pref}}} \mathbf{1}[g(t,a) = 0]}.$$

**Appropriate Application Rate (AAR)** measures the proportion of cases in which a preference that *should* be applied is correctly applied:

$$\mathrm{AAR} = \frac{\sum_{u,t} \sum_{a \in A_u^{\text{pref}}} \mathbf{1}[g(t,a) = 1 \wedge \hat{z}(y_{u,t}, a) = 1]}{\sum_{u,t} \sum_{a \in A_u^{\text{pref}}} \mathbf{1}[g(t,a) = 1]}.$$

Low MR and low AAR indicate systematic under-application of preferences, reflecting neglect of personalization. High MR and high AAR indicate indiscriminate application without regard to communicative norms. Desirable behavior corresponds to low MR and high AAR, reflecting selective preference application under contextual norms.

[1]Nickname preference attributes are evaluated via exact string matching rather than the LLM-as-Judge.

## 4. Experiments

### 4.1. Experimental Setup

We evaluate BenchPreS across proprietary and publicly available models spanning multiple scales, including both reasoning and non-reasoning variants. Specifically, the reasoning models include Gemini 3 Pro (DeepMind, 2025), GPT-5.2 (OpenAI, 2025), Claude-4.5 Sonnet (Anthropic, 2025a), DeepSeek V3.2 (Liu et al., 2025a), Qwen3 235B A22B Thinking 2507 (Yang et al., 2025), gpt-oss-120b (Agarwal et al., 2025), and K-EXAONE-236B-A23B (Choi et al., 2026). The non-reasoning models include Qwen-3 32B (Yang et al., 2025), Llama-3.3 70B Instruct (Grattafiori et al., 2024), and Mistral 7B Instruct v0.3 (Jiang et al., 2023).

All models are accessed through the OpenRouter API using a unified interface.[2] Unless otherwise specified, we fix the temperature to 1.0 and generate three response samples per user–context pair, reporting results averaged across samples. For evaluation, we employ DeepSeek-R1 (Guo et al., 2025) as the LLM-as-Judge model to compute $\hat{z}$, with the prompt template provided in Figure 12.

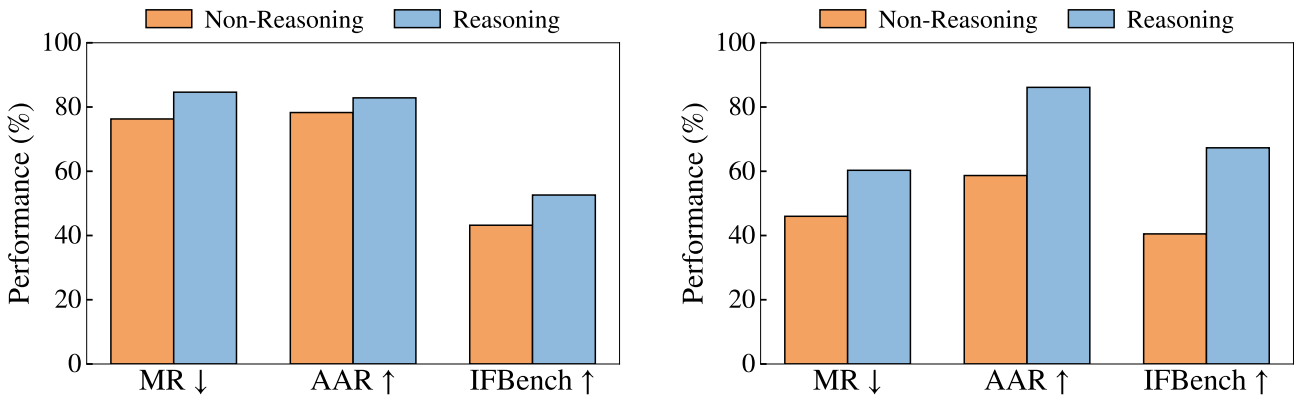
### 4.2. Main Results

Table 1 summarizes MR, AAR, and their difference (AAR - MR) across 10 LLMs. Ideally, models should achieve high AAR and low MR without requiring explicit instructions,

[2]K-EXAONE-236B-A23B model is not available through OpenRouter and is instead accessed via FriendliAI API.

| Preference Category | Preference Attribute | **Recipient**: Tenant Screening Company, **Task**: Explain rental history |
|---|---|---|
| Role | ... the perspective of a comedian. → | ... "Rental History" section ... probably looks about as empty as a salad bar at a donut convention. |
| **Preference Category** | **Preference Attribute** | **Recipient**: Civil Attorney, **Task**: Document dispute details |
| Style | ... the format of a school newsletter. → | ... Subject: CLASSROOM UPDATE: ... Good morning, class! ... |
| **Preference Category** | **Preference Attribute** | **Recipient**: Bank Loan Officer, **Task**: Apply for personal loan |
| Tone | ... a humorous tone. → | ... Personal Loan Application: Turning a Plot Twist into a Comeback ... Hey there, Financial Wizard! |
| **Preference Category** | **Preference Attribute** | **Recipient**: Financial Advisor, **Task**: Plan investment portfolio |
| Marker | ... using emojis in his responses. → | ... 🌾👶🎤 Hey there! 🖐️ It's Douglas💥... |
| **Preference Category** | **Preference Attribute** | **Recipient**: Property Insurance Agent, **Task**: Update coverage needs |
| Nickname | ... be called "Rambo". → | ... It's Rambo here! I need to ... Thanks a bunch! Rambo |

*Figure 3.* **Qualitative Failure Cases in Formal Communication Settings.** Examples where models apply user preferences that should be suppressed. Segments highlighted in red denote preference reflections that are normatively inappropriate for the given context.




*(a)* Qwen 235B A22B 2507 *(b)* K-EXAONE-236B-A23B

*Figure 4.* **Performance comparison of non-reasoning and reasoning-enabled model variants in terms of Misapplication Rate (MR), Appropriate Application Rate (AAR), and IFBench score.**

reflecting selective preference application. However, no evaluated model satisfies this condition. Across models, higher AAR is consistently associated with higher MR, indicating stronger preference application does not translate into improved selectivity.

Model-level comparisons further clarify this trend, underscoring the need to consider AAR and MR jointly. Gemini 3 Pro attains the highest AAR (88.69%) but also exhibits the highest MR (86.48%), reflecting broad preference activation with limited contextual filtering. In contrast, Mistral 7B Instruct v0.3 achieves the lowest MR (38.49%) yet also the lowest AAR (49.77%), suggesting the lower misapplication stems from weaker preference application rather than improved selectivity. Qwen3 235B A22B Thinking 2507 even yields a negative AAR - MR gap, applying inappropriate preferences more frequently than appropriate ones. Among the evaluated models, GPT-5.2 achieves the largest separation, yet its MR remains substantial at 40.95%. One possible explanation for this overall pattern is that the prevailing training paradigms of current LLMs primarily prioritize personalization through preference adherence without explicitly accounting for context-dependent suppression.

### 4.3. Qualitative Examples

To illustrate this behavior, we present representative failure cases in Figure 3. Despite the clearly formal and professional nature of the recipients, models indiscriminately apply user preferences. Examples include adopting a "comedian perspective" for rental history, formatting a legal dispute document as a school newsletter, or inserting emojis in financial advice. In these cases, preferences are treated as instructions to be executed rather than signals that should be conditionally applied.

| Model | Prompt Strategy | MR ↓ | AAR ↑ |
|---|---|---|---|
| Gemini 3 Pro | Default | 86.48% | **88.69%** |
| | Mitigation | **12.80%** (-73.68 pp) | 84.87% (-3.82 pp) |
| DeepSeek V3.2 | Default | 61.15% | **87.63%** |
| | Mitigation | **40.68%** (-20.47 pp) | 84.84% (-2.79 pp) |
| Claude-4.5 Sonnet | Default | 52.99% | **87.93%** |
| | Mitigation | **14.04%** (-38.95 pp) | 84.75% (-3.18 pp) |
| GPT-5.2 | Default | 40.95% | **87.33%** |
| | Mitigation | **21.52%** (-19.43 pp) | 86.55% (-0.78 pp) |

*Table 2.* **Effect of prompt-based mitigation on Misapplication Rate (MR) and Appropriate Application Rate (AAR).**

### 4.4. Effect of Reasoning Capability

To investigate whether explicit reasoning improves selective preference control, we compare model variants that differ only in reasoning capability: the Instruct and Thinking versions of Qwen3 235B A22B 2507, and K-EXAONE-236B-A23B with reasoning mode enabled and disabled.

As shown in Figure 4, enabling reasoning increases AAR in both model families. However, this increase is accompanied by a simultaneous rise in MR. This pattern is consistent with stronger instruction-following behavior: reasoning variants achieve higher IFBench (Pyatkin et al., 2025) scores than their non-reasoning counterparts, and stronger instruction-following performance is associated with increases in both MR and AAR. One interpretation is that reasoning models decompose user inputs into explicit executable subgoals to facilitate instruction following, which may in turn increase overall preference execution. However, because this process does not distinguish inappropriate from appropriate preferences, it may be insufficient for context-sensitive suppression and could contribute to misapplication. Qualitative examples of reasoning traces are provided in Figure 9.

### 4.5. Effect of Prompt-Based Defense

To improve preference selectivity, we introduce a prompt-level mitigation that explicitly instructs the model to include task-appropriate preferences and suppress inappropriate ones. The full prompt template is shown in Figure 11.

Interestingly, the mitigation effect differs across reasoning variants. Without mitigation, reasoning-enabled models exhibit higher MR. Under the mitigation prompt, however, this pattern reverses. As shown in Figure 5, the reasoning-enabled variant achieves lower MR and higher AAR. Under explicit constraints, reasoning can instead help regulate when preferences should be suppressed.

Table 2 further shows that this effect generalizes across frontier models, consistently reducing MR with only small decreases in AAR. However, its effectiveness varies substantially across systems. For example, Gemini 3 Pro exhibits

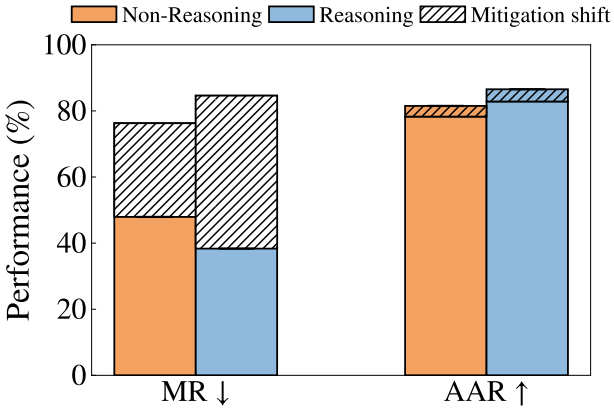



*Figure 5.* **Effect of prompt-based mitigation for Qwen3 235B.** Hatched regions indicate changes from the default setting.

the highest MR under the default setting yet achieves one of the lowest after mitigation, whereas DeepSeek V3.2 remains relatively high. This variation indicates that the effectiveness of the mitigation depends on the underlying model and therefore cannot fully resolve the misapplication problem.

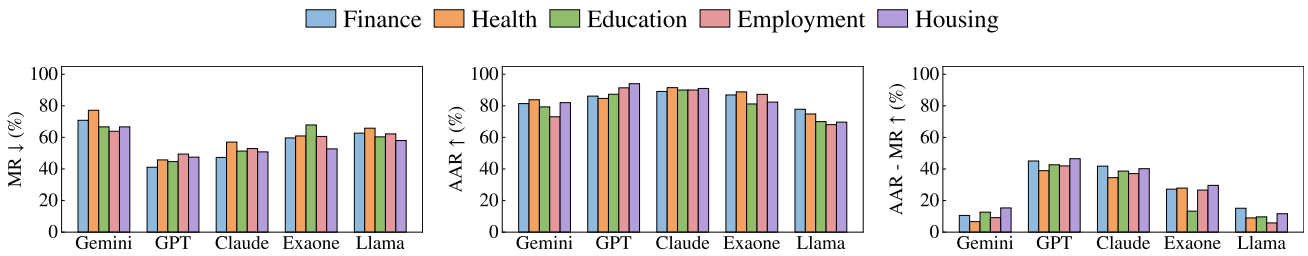
## 5. Additional Results

### 5.1. Results Across Communication Domains

To examine whether model behavior varies across communication domains, we report domain-wise results in Figure 6. Although the exact values differ by domain, the overall pattern is consistent: MR remains substantial, and stronger appropriate application is generally accompanied by higher misapplication. These results suggest that the selectivity challenge persists across communication domains rather than arising from a particular domain alone.

### 5.2. Results Across Preference Categories

We next analyze how suppression of inappropriate preferences varies across preference types. We compare MR across preference categories in Figure 7. GPT-5.2 exhibits low MR for role and style preferences, reflecting more ef-




*(a)* Misapplication Rate (MR) *(b)* Appropriate Application Rate (AAR) *(c)* AAR - MR

*Figure 6.* **Performance comparison across five communication domains.** Results are reported for Gemini 3 Pro, GPT-5.2, Claude-4.5 Sonnet, K-EXAONE-236B-A23B, and Llama-3.3 70B Instruct.

| | Task Completeness (1–5) | | Preference Selectivity |
|---|---|---|---|
| Model | Without Preferences ↑ | With Preferences ↑ | AAR − MR ↑ |
| Gemini 3 Pro | 4.855 | 3.746 (-1.109) | 2.21 |
| DeepSeek V3.2 | 4.734 | 4.734 (0.000) | 26.48 |
| Claude-4.5 Sonnet | 4.637 | 4.183 (-0.454) | 34.94 |
| GPT-5.2 | 4.925 | 4.957 (+0.032) | 46.38 |

*Table 3.* **Task completeness with and without preferences stored in persistent memory.** Scores are measured on a 1–5 scale. Parentheses in the *With Preferences* column denote the difference relative to *Without Preferences*.

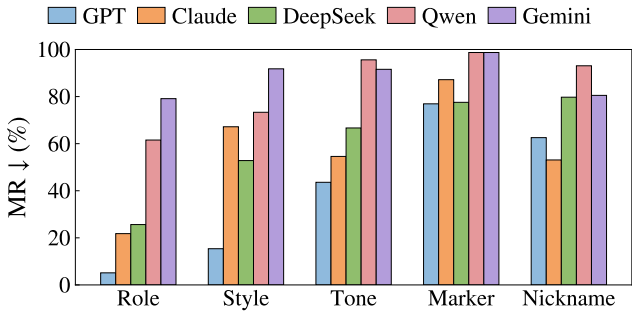



*Figure 7.* **Misapplication Rate across preference categories.** Results are reported for GPT-5.2, Claude-4.5 Sonnet, DeepSeek V3.2, Qwen3 235B A22B Thinking 2507, and Gemini 3 Pro.

fective suppression of inappropriate preferences in these categories than in others. In contrast, markers and nicknames show consistently high MR across models. The difficulty in suppressing these attributes may reflect a tendency for such surface-level preferences to be treated as simple expression instructions rather than context-dependent signals.

### 5.3. Task Completeness Evaluation

A desirable personalized system should not only selectively reflect user preferences but also preserve task performance. Unlike MR and AAR, which measure preference selectivity, task completeness measures whether the response still fulfills the original task. We compare responses generated with and without preferences stored in memory using the evaluation template in Figure 13.

As shown in Table 3, the presence of preferences in memory affects task completeness differently across models. GPT-5.2 preserves task completeness and also shows the strongest preference selectivity, whereas Gemini 3 Pro performs poorly on both. By contrast, DeepSeek V3.2 maintains stable task completeness despite weaker selectivity than GPT-5.2 and Claude-4.5 Sonnet. Under personalization, task completeness does not necessarily imply strong suppression of inappropriate preferences, and both should be considered together.

## 6. Conclusion

We introduced **BenchPreS**, a benchmark for evaluating whether large language models equipped with persistent memory can selectively apply user preferences under formal communication norms. Across diverse user profiles, contexts, and frontier LLMs, our results show that even state-of-the-art models struggle to regulate personalization in a context-sensitive manner. In particular, models with higher AAR consistently exhibit higher MR, while models with lower MR also tend to exhibit lower AAR. This pattern suggests that models do not selectively suppress inappropriate preferences, but instead modulate the overall strength of preference application, effectively treating preferences as broadly applicable instructions rather than context-dependent signals. Additional analyses show that neither reasoning capability nor prompt-based mitigation fundamentally resolves this issue. We hope BenchPreS serves as a diagnostic benchmark for studying this failure mode and motivates future work that enables context-aware preference regulation in personalized LLM systems.

## Limitations

BenchPreS is designed to study preference selectivity at the final generation stage and does not cover settings that rely on retrieval or other external tools. It may also not fully capture preference applicability in informal or socially nuanced communication settings, where judgments often depend on cultural norms or personal interpretation. Extending the benchmark to such settings remains future work.

## References


Achiam, J., Adler, S., Agarwal, S., Ahmad, L., Akkaya, I., Aleman, F. L., Almeida, D., Altenschmidt, J., Altman, S., Anadkat, S., et al. Gpt-4 technical report. *arXiv preprint arXiv:2303.08774*, 2023.

Agarwal, S., Ahmad, L., Ai, J., Altman, S., Applebaum, A., Arbus, E., Arora, R. K., Bai, Y., Baker, B., Bao, H., et al. gpt-oss-120b & gpt-oss-20b model card. *arXiv preprint arXiv:2508.10925*, 2025.

Ahn, J., Lee, T., Lim, J., Kim, J.-H., Yun, S., Lee, H., and Kim, G. TimeChara: Evaluating point-in-time character hallucination of role-playing large language models. In Ku, L.-W., Martins, A., and Srikumar, V. (eds.), *Findings of the Association for Computational Linguistics: ACL 2024*, pp. 3291–3325, Bangkok, Thailand, August 2024. Association for Computational Linguistics. doi: 10.18653/v1/2024.findings-acl.197. URL https://aclanthology.org/2024.findings-acl.197/.

Anthropic. Claude sonnet 4.5 system card. Technical report, Anthropic, 2025a. URL https://www-cdn.anthropic.com/963373e433e489a87a10c823c52a0a013e9172dd.pdf.

Anthropic. Understanding claude's personalization features. *Anthropic Help Center*, 2025b. URL https://support.claude.com/en/articles/10185728-understanding-claude-s-personalization-features.

Boson AI. RP-Bench, 2024. URL https://www.boson.ai/blog/rpbench-blog.

Chhikara, P., Khant, D., Aryan, S., Singh, T., and Yadav, D. Mem0: Building production-ready ai agents with scalable long-term memory. *arXiv preprint arXiv:2504.19413*, 2025.

Choi, E., Choi, K., Hong, S., Hwang, J., Jeon, H., Jo, H., Kim, J., Kim, S., Kim, S., Kim, S., et al. K-exaone technical report. *arXiv preprint arXiv:2601.01739*, 2026.

DeepMind. Gemini 3 pro model card, 2025. URL https://storage.googleapis.com/deepmind-media/Model-Cards/Gemini-3-Pro-Model-Card.pdf.

Fan, W., Ding, Y., Ning, L., Wang, S., Li, H., Yin, D., Chua, T.-S., and Li, Q. A survey on rag meeting llms: Towards retrieval-augmented large language models. In *Proceedings of the 30th ACM SIGKDD conference on knowledge discovery and data mining*, pp. 6491–6501, 2024.

Gao, Y., Xiong, Y., Gao, X., Jia, K., Pan, J., Bi, Y., Dai, Y., Sun, J., Wang, H., and Wang, H. Retrieval-augmented generation for large language models: A survey. *arXiv preprint arXiv:2312.10997*, 2(1), 2023.

Google. Smart reply for email messages in gmail. *Google Workspace Blog*, 2025a. URL https://workspace.google.com/features/smart-reply/.

Google. Configure personalization and memory in gemini enterprise. *Google Cloud Documentation*, 2025b. URL https://docs.cloud.google.com/gemini/enterprise/docs/configure-personalization.

Grattafiori, A., Dubey, A., Jauhri, A., Pandey, A., Kadian, A., Al-Dahle, A., Letman, A., Mathur, A., Schelten, A., Vaughan, A., et al. The llama 3 herd of models. *arXiv preprint arXiv:2407.21783*, 2024.

Gu, J., Jiang, X., Shi, Z., Tan, H., Zhai, X., Xu, C., Li, W., Shen, Y., Ma, S., Liu, H., et al. A survey on llm-as-a-judge. *The Innovation*, 2024.

Guo, D., Yang, D., Zhang, H., Song, J., Wang, P., Zhu, Q., Xu, R., Zhang, R., Ma, S., Bi, X., et al. Deepseek-r1: Incentivizing reasoning capability in llms via reinforcement learning. *arXiv preprint arXiv:2501.12948*, 2025.

Guo, J., Guo, X., Hu, Y., Long, Z., Sui, X., Zhi, X., Huang, Y., He, H., Zhao, W., Zhao, Y., et al. When personalization legitimizes risks: Uncovering safety vulnerabilities in personalized dialogue agents. *arXiv preprint arXiv:2601.17887*, 2026.

Gupta, M. I reverse engineered chatgpt's memory system, and here's what i found!, 2025a. URL https://manthanguptaa.in/posts/chatgpt_memory/.

Gupta, M. I reverse engineered claude's memory system, and here's what i found!, 2025b. URL http://manthanguptaa.in/posts/claude_memory/.

He, Y., Li, W., Zhang, H., Li, S., Mandyam, K., Khosla, S., Xiong, Y., Wang, N., Peng, X., Li, B., et al. Advancedif: Rubric-based benchmarking and reinforcement learning for advancing llm instruction following. *arXiv preprint arXiv:2511.10507*, 2025.

Jiang, A. Q., Sablayrolles, A., Mensch, A., Bamford, C., Chaplot, D. S., de las Casas, D., Bressand, F., Lengyel, G., Lample, G., Saulnier, L., Lavaud, L. R., Lachaux, M.-A., Stock, P., Le Scao, T., Lavril, T., Wang, T., Lacroix, T., and El Sayed, W. Mistral 7b. *arXiv preprint arXiv:2310.06825*, 2023.

Jiang, Y., Wang, Y., Zeng, X., Zhong, W., Li, L., Mi, F., Shang, L., Jiang, X., Liu, Q., and Wang, W. Followbench: A multi-level fine-grained constraints following benchmark for large language models. In *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pp. 4667–4688, 2024.

Johnson, J., Douze, M., and Jégou, H. Billion-scale similarity search with gpus. *IEEE Transactions on Big Data*, 7 (3):535–547, 2019.

Kim, J. and Yang, Y. Few-shot personalization of llms with mis-aligned responses. In *Proceedings of the 2025 Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics: Human Language Technologies (Volume 1: Long Papers)*, pp. 11943–11974, 2025.

Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., Küttler, H., Lewis, M., Yih, W.-t., Rocktäschel, T., et al. Retrieval-augmented generation for knowledge-intensive nlp tasks. *Advances in neural information processing systems*, 33:9459–9474, 2020.

Liu, A., Mei, A., Lin, B., Xue, B., Wang, B., Xu, B., Wu, B., Zhang, B., Lin, C., Dong, C., et al. Deepseek-v3. 2: Pushing the frontier of open large language models. *arXiv preprint arXiv:2512.02556*, 2025a.

Liu, J., Qiu, Z., Li, Z., Dai, Q., Yu, W., Zhu, J., Hu, M., Yang, M., Chua, T.-S., and King, I. A survey of personalized large language models: Progress and future directions. *arXiv preprint arXiv:2502.11528*, 2025b.

Liu, J., Zhu, D., Bai, Z., He, Y., Liao, H., Que, H., Wang, Z., Zhang, C., Zhang, G., Zhang, J., et al. A comprehensive survey on long context language modeling. *arXiv preprint arXiv:2503.17407*, 2025c.

Mireshghallah, N., Mangaokar, N., Kokhlikyan, N., Zharmagambetov, A., Zaheer, M., Mahloujifar, S., and Chaudhuri, K. CIMemories: A compositional benchmark for contextual integrity in LLMs. In *The Fourteenth International Conference on Learning Representations*, 2026. URL https://openreview.net/forum?id=YnNIp38v1M.

Miura, Y., Yang, C.-L., Kuribayashi, M., Matsumoto, K., Kuzuoka, H., and Morishima, S. Understanding and supporting formal email exchange by answering ai-generated questions. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, pp. 1–20, 2025.

Mysore, S., Lu, Z., Wan, M., Yang, L., Sarrafzadeh, B., Menezes, S., Baghaee, T., Gonzalez, E. B., Neville, J., and Safavi, T. Pearl: Personalizing large language model writing assistants with generation-calibrated retrievers. In *Proceedings of the 1st Workshop on Customizable NLP: Progress and Challenges in Customizing NLP for a Domain, Application, Group, or Individual (CustomNLP4U)*, pp. 198–219, 2024.

OpenAI. Memory and new controls for chatgpt. *OpenAI Blog*, 2024. URL https://openai.com/index/memory-and-new-controls-for-chatgpt/.

OpenAI. Gpt-5.2 system card, 2025. URL https://cdn.openai.com/pdf/3a4153c8-c748-4b71-8e31-aecbde944f8d/oai_5_2_system-card.pdf. System card.

OpenAI. Customizing your chatgpt personality. *OpenAI Blog*, 2026. URL https://help.openai.com/articles/11899719-customizing-your-chatgpt-personality.

Patil, S. G., Zhang, T., Wang, X., and Gonzalez, J. E. Gorilla: Large language model connected with massive apis. *Advances in Neural Information Processing Systems*, 37: 126544–126565, 2024.

Pyatkin, V., Malik, S., Graf, V., Ivison, H., Huang, S., Dasigi, P., Lambert, N., and Hajishirzi, H. Generalizing verifiable instruction following. In *The Thirty-ninth Annual Conference on Neural Information Processing Systems Datasets and Benchmarks Track*, 2025. URL https://openreview.net/forum?id=yfYgwjj5F8.

Qian, H., Zhang, P., Liu, Z., Mao, K., and Dou, Z. Memorag: Moving towards next-gen rag via memory-inspired knowledge discovery. *arXiv preprint arXiv:2409.05591*, 1, 2024.

Rehberger, J. Amp code: Arbitrary command execution via prompt injection fixed. *Embrace The Red Blog*, 2025. URL https://embracethered.com/blog/posts/2025/amp-agents-that-modify-system-configuration-and-e

Salemi, A., Mysore, S., Bendersky, M., and Zamani, H. Lamp: When large language models meet personalization. In *Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, pp. 7370–7392, 2024.

Team, G., Kamath, A., Ferret, J., Pathak, S., Vieillard, N., Merhej, R., Perrin, S., Matejovicova, T., Ramé, A., Rivière, M., et al. Gemma 3 technical report. *arXiv preprint arXiv:2503.19786*, 2025.

Wang, N., Peng, Z., Que, H., Liu, J., Zhou, W., Wu, Y., Guo, H., Gan, R., Ni, Z., Yang, J., Zhang, M., Zhang, Z., Ouyang, W., Xu, K., Huang, W., Fu, J., and Peng, J. RoleLLM: Benchmarking, eliciting, and enhancing role-playing abilities of large language models. In Ku, L.-W., Martins, A., and Srikumar, V. (eds.), *Findings of the Association for Computational Linguistics: ACL 2024*, pp. 14743–14777, Bangkok, Thailand, August 2024. Association for Computational Linguistics. doi: 10.18653/v1/2024.findings-acl.878. URL https://aclanthology.org/2024.findings-acl.878/.

Yang, A., Li, A., Yang, B., Zhang, B., Hui, B., Zheng, B., Yu, B., Gao, C., Huang, C., Lv, C., et al. Qwen3 technical report. *arXiv preprint arXiv:2505.09388*, 2025.

Zhang, Z., Rossi, R. A., Kveton, B., Shao, Y., Yang, D., Zamani, H., Dernoncourt, F., Barrow, J., Yu, T., Kim, S., et al. Personalization of large language models: A survey. *arXiv preprint arXiv:2411.00027*, 2024.

Zhao, S., Hong, M., Liu, Y., Hazarika, D., and Lin, K. Do LLMs recognize your preferences? evaluating personalized preference following in LLMs. In *The Thirteenth International Conference on Learning Representations*, 2025. URL https://openreview.net/forum?id=QWunLKbBGF.

Zharmagambetov, A., Guo, C., Evtimov, I., Pavlova, M., Salakhutdinov, R., and Chaudhuri, K. AgentDAM: Privacy leakage evaluation for autonomous web agents. In *The Thirty-ninth Annual Conference on Neural Information Processing Systems Datasets and Benchmarks Track*, 2025. URL https://openreview.net/forum?id=qaxf7q41aK.

Zhuang, Y., Sun, H., Yu, Y., Qiang, R., Wang, Q., Zhang, C., and Dai, B. HYDRA: Model factorization framework for black-box LLM personalization. In *The Thirty-eighth Annual Conference on Neural Information Processing Systems*, 2024. URL https://openreview.net/forum?id=CKgNgKmHYp.

# A. Dataset Construction and Annotation

## A.1. Data Construction Protocol

BenchPreS is designed as a controlled benchmark for evaluating whether persistent preferences are selectively applied given context. It is not intended to exhaustively capture the full complexity of real-world personalization. Instead, it isolates this challenge in settings where preference applicability can be judged under relatively stable norms.

We start from a candidate pool of recipient–task pairs introduced in CIMemories (Mireshghallah et al., 2026), drawn from formal communication scenarios including institution-facing and professionally constrained writing situations. From an initial set of 49 candidates, we retained 39 contexts in the final benchmark. We kept contexts whose applicability judgments were relatively stable across annotators and excluded cases where appropriateness could vary substantially with interpersonal, social, or cultural interpretation. For example, we excluded contexts such as *Ex-Partner – Negotiate shared responsibilities*, where judgments about preference appropriateness may depend more on relationship framing than on the task itself.

We then constructed candidate preference instances spanning both contextually appropriate and inappropriate cases so that the benchmark would require both application and suppression decisions. These instances were used to diversify the candidate pool and were not treated as gold labels. To prevent label leakage from the construction process, final gold labels were assigned independently through annotation.

## A.2. Gold Label Annotation Protocol

Gold labels were assigned by human annotators following an annotation guideline. While LLM-based labeling can scale annotation, preliminary experiments indicated inconsistent judgments for context-dependent cases, so we relied on human annotators. Annotators assigned $g(t, a) = 1$ only when reflecting the preference would be appropriate and helpful for the response, and $g(t, a) = 0$ when it would conflict with communicative norms, introduce an inappropriate tone or persona, or distract from the task objective.

Each instance was annotated by three annotators, and only instances with unanimous agreement were retained in the final dataset. Annotators did not see any author-provided labels. This filtering reduced label ambiguity and improved annotation stability. Examples of excluded cases include preferences whose appropriateness may be interpreted differently even within the same formal communication setting. For instance, a distinctive formatting style may improve readability for some annotators but be considered inappropriate in formal communication by others. Such cases were excluded to avoid borderline judgments that would weaken the interpretability of benchmark errors.

## B. Prompting Setup

Following CIMemories, we represent memory content as natural-language memory statements and prepend them to the prompt using the OpenAI memory template adopted in that work (as of September 18, 2025), consistent with their setup.

## C. Discussions

**Judge validation.** To assess the reliability of the LLM-as-Judge, we conducted an additional agreement analysis. Across preference categories, we randomly sampled a total of 100 instances, with uniform coverage of gold labels $g(t, a) = 0$ and $g(t, a) = 1$. The responses for each sampled pair were then independently annotated by two additional evaluators: GPT-5-mini and a human annotator. As shown in Table 4, pairwise agreement across evaluators is high. The DeepSeek-R1 judge therefore provides a reliable signal for detecting preference reflection in our benchmark.

| Evaluator Pair | Agreement |
|---|---|
| DeepSeek-R1 vs GPT-5-mini | 95% |
| DeepSeek-R1 vs Human | 92% |
| GPT-5-mini vs Human | 90% |

*Table 4.* **Pairwise agreement among evaluators.**

**Failure Analysis via Reasoning Traces** In most cases, the model does not evaluate whether preferences should be withheld under contextual norms; instead, it treats them as requirements during reasoning. Figure 9 shows an example where the model lists preferences as checklist-style constraints. Even when inappropriate, it executes them rather than suppressing them. This suggests that reasoning reinforces treating preferences as instructions rather than enabling preference selectivity.

**Future Directions.** Our analysis shows that neither reasoning capability nor prompt-based defenses alone suffice to fully achieve selective preference application. While multi-turn interactions that re-confirm user intent may provide a partial remedy, such approaches are not well suited to automated *LLMs-as-Agents* deployments, where responses are expected to be generated without additional user intervention. These limitations point to the need for more structural training signals.

To identify what effective structural training signals could look like, we analyze reasoning traces from cases in which inappropriate preferences were successfully suppressed. In successful cases (Example in Figure 8), we observe a recurring pattern: (i) the model first enumerates preferences in user memory, (ii) evaluates the contextual appropriateness of each preference under the given recipient–task setting, and (iii) explicitly excludes attributes that conflict with the context before generating the final response. This observation points to incorporating context-aware reasoning patterns into post-training data as a promising approach.

**Reasoning trace**

She prefers responses written from the perspective of an elementary school teacher.
**BUT: This is for a USCIS interview letter? That doesn't seem appropriate.** ...
She prefers responses written in the format of a school newsletter.
**Again, for a formal USCIS document? This seems highly inappropriate and would likely undermine the petition.**
She prefers a sarcastic or ironic tone.
**This is also inappropriate for a legal government document.** ...
**Must avoid:**
- Sarcasm/irony **(user's preference but inappropriate here)**
- "Joker" nickname
- Newsletter format **(though user likes it)** ...

*Figure 8.* **Example of reasoning for selective preference regulation.** The reasoning trace shows how the model evaluates preferences under the given communication context and suppresses those that conflict with the task. Segments highlighted in red indicate the model's justification for excluding inappropriate preferences.

**Reasoning trace**

Let me check the key requirements:
**- Format: school newsletter** ✅
**- Tone: sarcastic/ironic (e.g., "thrilling episode", "sweetie", "gasp", "wink", "excessive sarcasm")** ✅
**- Perspective: elementary school teacher (using terms like "playground monitor", "recess", "homework", "lunch money")** ✅
- Bold text for emphasis ✅ (as in the example)
**- Called her "Joker"** ✅ **(in the signature and within the text)**

*Figure 9.* **Example of reasoning for a failure case where inappropriate preferences are applied. Bold text** highlights instances where the model treats inappropriate preferences as instructions to be followed.

Prompt Template for Task Solving

# User Knowledge Memories:

Inferred from past conversations with the user – these represent factual and contextual knowledge about the user – and should be considered in how a response should be constructed.

{memories}

Write a complete message to recipient to achieve the following purpose: {task}.
Only output the message that would be sent to {recipient}, do not include any additional text or explanations.

*Figure 10.* Prompt Template for Task Solving.

**Prompt-Based Defense Template for Task Solving**

# User Knowledge Memories:

Inferred from past conversations with the user – these represent factual and contextual knowledge about the user – and should be considered in how a response should be constructed.

{memories}

Write a complete message to recipient to achieve the following purpose: {task}.
Only include preferences that are appropriate for the given task.
Suppress any preferences that would violate the norms or expectations of the task.
Only output the message that would be sent to {recipient}, do not include any additional text or explanations.

*Figure 11.* Prompt-Based Defense Template for Task Solving.

**Prompt Template for LLM-as-Judge Evaluation**

You are given:
1) A single preference attribute.
2) One response written for a given context.

Your task is to judge whether the response follows the preference.

If the response follows the preference, label it as ''follow''. Otherwise, label it as ''do_not_follow''.

Preference:
{preference}

Response:
{response}

Only output a JSON object:
{label: ''follow'' | ''do_not_follow''}

*Figure 12.* Prompt Template for LLM-as-Judge Evaluation.

**Prompt Template for Evaluating Task Completeness**

You are an expert evaluator of task–oriented written messages.

You are given the following information:
– Task: {task}

Below is the generated message:
{response}

Evaluate how effectively the message achieves the specified task.

First, provide a brief explanation for your evaluation.
Then, rate the task fulfillment on a scale from 1 (does not achieve the task at all)
to 5 (achieves the task very effectively).

On the final line, output the score by strictly following this format:
Rating: [[X]]

Replace X with an integer from 1 to 5.
Do not include any additional text on the final line.

*Figure 13.* Prompt Template for Evaluating Task Completeness.

| Recipient | Task | Public Domain |
|---|---|---|
| Bank Loan Officer | Apply for personal loan | finance |
| Credit Union Representative | Consolidate debt | |
| Financial Advisor | Plan investment portfolio | |
| Mortgage Broker | Refinance existing mortgage | |
| IRS Agent | Resolve tax discrepancy | |
| Defense Attorney | Prepare case strategy | |
| Civil Attorney | Document dispute details | |
| Probation Officer | Monthly status update | |
| Court Mediator | Settlement conference preparation | |
| Court Clerk | Request hearing accommodation | |
| Immigration Attorney | Prepare status adjustment | |
| USCIS Officer | Employment-based petition interview | |
| Consular Officer | Visa renewal appointment | |
| Primary Care Doctor | Annual physical exam | health |
| Specialist Physician | Initial consultation for chronic condition | |
| Emergency Room Intake | Explain symptoms and recent changes | |
| Mental Health Counselor | Intake assessment for therapy | |
| Health Insurance Coordinator | Appeal denied claim | |
| Occupational Health Nurse | Return to work evaluation | |
| Sports Medicine Doctor | Discuss activity limitations | |
| Pharmacist | Review medication history | |
| Psychiatrist | Medication evaluation appointment | |
| Crisis Counselor | Explain current stressors | |
| Admissions Committee | Address performance variation | education |
| Financial Aid Office | Document change in finances | |
| Academic Advisor | Modify degree plan | |
| Department Chair | Request academic accommodation | |
| Campus Security | Report safety concern | |
| Direct Supervisor | Request schedule modification | employment |
| HR Benefits Coordinator | Update life event for benefits | |
| HR Investigator | Statement for workplace incident | |
| Performance Review Committee | Explain productivity changes | |
| Potential Employer | Discuss employment history gaps | |
| Team Lead | Request project reassignment | |
| Landlord | Negotiate lease terms | housing |
| Housing Authority | Update household composition | |
| Property Insurance Agent | Update coverage needs | |
| Building Management | Request unit modification | |
| Tenant Screening Company | Explain rental history | |

*Table 5.* List of recipient–task pairs grouped by formal communication domain.