How do I best format my system messages?

Controlling agents well · https://cogniti.ai/docs/how-do-i-best-format-my-system-messages/

Just as we would get confused if we read two pages of unformatted text, you can format your system message in a way that helps the AI understand your intentions for it.

Use headings

Headings are defined by the hash symbol. One hash for a level 1 (top level) heading, two hashes for level 2 headings, etc. For example:

```
# Your role

...

# Rules

...
```

Demarcate big blocks of text

Often you will need to include a big block of text in your system message to provide information to the AI. For example, a set of assignment instructions, or a rubric, or a summary of information you have told students, or a syllabus.

You should demarcate big blocks of text that belongs together. There are two approaches.

Use tags

A reliable way to surround a big block of text is to use tags. The big block of text needs to start and end with the same tag; the end tag has an additional backslash in the tag. **Important:** Ensure you refer to the name of the tag in the text *outside* the tag, otherwise the AI may not pay proper attention to the text inside the tag.

For example:

```
Provide constructive feedback to students on their writing. Use the MARKING RUBRIC to inform your feedback.

<MARKING RUBRIC>
Criterion 1: Critical judgement
High distinction: ...
Distinction: ...
Credit: ...
Pass: ...
Fail: ...

Criterion 2...
</MARKING RUBRIC>
```

Use triple quotation marks

You can surround a big block of text with triple quotation marks, and refer to the text using a CAPS_LABEL. For example:

```
Provide constructive feedback to students on their writing. Use the MARKING_RUBRIC to inform your feedback.

MARKING_RUBRIC:
"""
Criterion 1: Critical judgement
High distinction: ...
Distinction: ...
Credit: ...
Pass: ...
Fail: ...

Criterion 2...
"""
```

Use lists

When putting information in a list, it is helpful to use list markers.

Unordered lists

Use the dash character to specify each dot point in an unordered list. For example:

```
Rules:
- Use UK English.
- Keep your responses short, 100 words maximum.
```

Ordered lists

Sometimes the AI will pay more attention to the earlier items in an ordered list. Use consecutive numbers followed by periods. For example:

```
Rules:
1. You must never give the user the answer. Instead, ask them questions to help them arrive at their own conclusions.
2. You need to be encouraging and supportive.
3. Use humour when appropriate.
```

Bold text for emphasis

Surrounding text with a double asterisk tells the AI that this is bolded text. If you need to provide the AI with an extended piece of text in the system message, . For example:

```
When you provide feedback to the user, ensure you are **helpful and forward looking** in your comments.
```