

Số -QC/ĐU

QUY CHẾ

khai thác và sử dụng Trí tuệ nhân tạo (AI) đối với cán bộ, đảng viên, cá nhân trong hệ thống chính trị trên địa bàn phường Phước Bình

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11, ngày 29/6/2006;

Căn cứ Luật Cơ yếu số 05/2011/QH13, ngày 26/11/2011;

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13, ngày 19/11/2015;

Căn cứ Luật An ninh mạng số 24/2018/QH14, ngày 12/6/2018;

Căn cứ Luật Bảo vệ bí mật nhà nước số 29/2018/QH14, ngày 15/11/2018;

Căn cứ Nghị định Bảo vệ dữ liệu cá nhân số 13/2023/NĐ-CP, ngày 17/4/2023;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15, ngày 26/6/2025;

Căn cứ Kết luận số 126-KL/BTV, ngày 09/03/2026 của Ban Thường vụ Đảng ủy phường tại phiên họp thứ 31 ngày 25/02/2026;

Xét đề nghị của Văn phòng Đảng ủy,

Ban Thường vụ Đảng ủy phường ban hành Quy chế khai thác và sử dụng Trí tuệ nhân tạo (AI) đối với cán bộ, đảng viên, cá nhân trong hệ thống chính trị trên địa bàn phường Phước Bình, như sau:

CHƯƠNG I QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này áp dụng đối với việc khai thác, sử dụng các công cụ AI phục vụ công tác quản lý, hành chính, tổng hợp, truyền thông, phân tích dữ liệu và các nhiệm vụ không thuộc phạm vi bí mật nhà nước, đồng thời không bao gồm dữ liệu cá nhân nhạy cảm hoặc thông tin nội bộ chưa được phép chia sẻ lên môi trường bên ngoài.

Điều 2. Đối tượng áp dụng

Cán bộ, đảng viên, công chức, viên chức, người lao động trong hệ thống chính trị từ phường đến các Chi bộ trực thuộc.

Điều 3. Giải thích từ ngữ

1. Trí tuệ nhân tạo (AI): Là công nghệ giúp máy tính có thể thực hiện các công việc đòi hỏi trí tuệ của con người như: học hỏi, suy luận, nhận dạng, giao tiếp và giải quyết vấn đề.

2. Mô hình ngôn ngữ lớn (LLM): Là một dạng AI chuyên sâu về ngôn ngữ, được huấn luyện trên khối lượng dữ liệu văn bản khổng lồ, có khả năng hiểu và tạo ra ngôn ngữ tự nhiên của con người. Các công cụ chatbot phổ biến hiện nay như ChatGPT hay Gemini là các LLM, có thể trò chuyện, trả lời câu hỏi, viết văn bản một cách linh hoạt.

3. AI giải thích được (Explainable AI - XAI): Tập trung vào việc làm cho các mô hình AI trở nên minh bạch, cho phép con người hiểu rõ lý do đằng sau các quyết định hoặc dự đoán của máy, điều này rất quan trọng đối với trách nhiệm giải trình.

4. AI tổng quát (Artificial General Intelligence - AGI): Có khả năng thực hiện bất kỳ nhiệm vụ trí tuệ nào mà con người có thể thực hiện.

5. Hội tụ công nghệ: AI ngày càng được kết hợp sâu rộng với các công nghệ khác như Internet vạn vật (IoT), Blockchain (để tăng cường bảo mật và tin cậy) và mạng 5G (để xử lý dữ liệu tốc độ cao), tạo ra các hệ thống thông minh và phức tạp hơn.

CHƯƠNG II

NGUYÊN TẮC QUẢN LÝ VÀ SỬ DỤNG AI

Điều 4. Nguyên tắc chung

1. Hỗ trợ, không thay thế: Luôn xác định AI là công cụ hỗ trợ, giúp tăng tốc và nâng cao chất lượng công việc. AI không thể thay thế tư duy phản biện, năng lực chuyên môn, kinh nghiệm thực tiễn và trách nhiệm ra quyết định của cán bộ, đảng viên.

2. Bắt buộc phải kiểm chứng: Không tin tưởng tuyệt đối vào bất kỳ kết quả nào do AI tạo ra. Mọi dữ kiện, số liệu, trích dẫn chủ trương, chính sách của Đảng và pháp luật Nhà nước đều phải được kiểm tra, đối chiếu lại từ các nguồn thông tin chính thống.

3. Bảo mật là trên hết: Phải có ý thức phân loại mức độ nhạy cảm của thông tin trước khi đưa vào AI. Tuyệt đối không cung cấp thông tin thuộc danh mục bí mật nhà nước, dữ liệu cá nhân nhạy cảm cho các nền tảng AI công cộng, không rõ nguồn gốc.

4. Tuân thủ và trách nhiệm: Chấp hành nghiêm các quy định của Đảng, pháp luật của Nhà nước về an ninh mạng, sở hữu trí tuệ, và các chuẩn mực đạo đức, văn hóa. Cán bộ, đảng viên phải chịu trách nhiệm giải trình về quá trình và kết quả sử dụng AI trong công việc của mình.

5. Tôn trọng quyền sở hữu trí tuệ: Tuyệt đối không sử dụng AI để sao chép, đạo văn, vi phạm bản quyền hoặc tạo ra các sản phẩm phái sinh trái phép từ các tác phẩm được bảo hộ của người khác, cần nhận thức rõ rủi ro về quyền tác giả: Dữ liệu nhập vào (input) các hệ thống AI công cộng có thể bị mất quyền kiểm soát; sản phẩm do AI tạo ra (output) nên không có sự đóng góp sáng tạo đáng kể của con người sẽ không được pháp luật bảo hộ quyền tác giả. Do đó, cán bộ, đảng viên phải thận trọng khi xác lập quyền sở hữu đối với các văn bản, sản phẩm được tạo ra từ AI.

6. Không làm thay trách nhiệm cá nhân: Không sử dụng AI để né tránh trách nhiệm tham mưu, thẩm định, ký ban hành văn bản hoặc đưa ra nhận định chuyên môn thay cho cán bộ, đảng viên.

Điều 5. Yêu cầu sử dụng

1. Việc sử dụng AI phải đặt dưới sự lãnh đạo của Đảng, tuân thủ nghiêm ngặt các quy định của Đảng, pháp luật của Nhà nước, đặc biệt là các quy định về bảo vệ bí mật nhà nước, an ninh mạng và bảo vệ dữ liệu cá nhân.

2. Mọi thông tin, sản phẩm do AI tạo ra phải được cán bộ, đảng viên kiểm chứng, thẩm định, chỉnh sửa và chịu trách nhiệm hoàn toàn về nội dung trước khi sử dụng hoặc ban hành.

3. Tuyệt đối không phụ thuộc, lệ thuộc vào AI.

4. Ưu tiên sử dụng các nền tảng, giải pháp AI do Việt Nam phát triển và làm chủ (Make in Vietnam) khi xử lý các dữ liệu mang tính nội bộ, nhạy cảm nhằm đảm bảo an toàn, an ninh và chủ quyền dữ liệu quốc gia.

CHƯƠNG III PHẠM VI KHAI THÁC, SỬ DỤNG AI

Điều 6. Các trường hợp được phép sử dụng AI

1. Soạn thảo, gợi ý nội dung cho các văn bản, báo cáo không mật.
2. Hỗ trợ phân tích số liệu công khai hoặc dữ liệu không nhạy cảm.
3. Tự động hóa các tác vụ hành chính (lập kế hoạch, quản lý tiến độ, tổng hợp ý kiến...).
4. Hỗ trợ dịch thuật, tóm tắt tài liệu công khai.
5. Hỗ trợ thiết kế ấn phẩm truyền thông nội bộ, infographic, biểu đồ...

Điều 7. Các trường hợp tuyệt đối không được sử dụng AI

1. Soạn thảo văn bản liên quan đến nội dung mật, tối mật, tuyệt mật.
2. Nhập dữ liệu nhạy cảm, cá nhân, bảo mật lên AI công cộng.
3. Tạo và phát tán nội dung giả mạo (Deepfake).
4. Vi phạm quy tắc quản lý tài khoản và mật khẩu.
5. Lưu mật khẩu tại nơi công cộng.
6. Kết nối trái phép hệ thống nội bộ.
7. Đề xuất vấn đề thuộc thẩm quyền lãnh đạo, quyết định chính trị hoặc công tác tổ chức – cán bộ.
8. Sử dụng AI để tạo, chỉnh sửa nội dung xuyên tạc chủ trương của Đảng, chính sách pháp luật của Nhà nước hoặc cung cấp thông tin sai sự thật.

9. Tự ý sử dụng AI để phân tích hồ sơ cán bộ, hồ sơ đảng viên hoặc dữ liệu nhân sự khi chưa được cấp có thẩm quyền cho phép.

10. Đưa lên các nền tảng AI do tổ chức, cá nhân bên ngoài cung cấp nội dung dự thảo văn bản của Đảng, báo cáo nội bộ, tài liệu họp, tài liệu xin ý kiến khi chưa được phép công khai.

CHƯƠNG IV BẢO MẬT VÀ AN TOÀN THÔNG TIN

Điều 8. Yêu cầu về bảo vệ dữ liệu và an toàn thông tin

Cán bộ, đảng viên phải tự hình thành thói quen phân loại mức độ nhạy cảm của thông tin trước khi tương tác với bất kỳ hệ thống AI nào.

- **Cấp độ 1 (Công khai):** Thông tin đã được công bố trên các phương tiện thông tin đại chúng, cổng thông tin điện tử chính thức. *Có thể sử dụng các nền tảng AI do tổ chức, cá nhân bên ngoài cung cấp để xử lý.*

- **Cấp độ 2 (Nội bộ):** Thông tin lưu hành trong nội bộ cơ quan, không chứa bí mật nhà nước, chỉ được sử dụng nền tảng AI do tổ chức, cá nhân bên ngoài cung cấp khi đã loại bỏ toàn bộ thông tin định danh, thông tin nhạy cảm và không thể truy ngược lại nguồn dữ liệu. *Hạn chế sử dụng AI công cộng, ưu tiên các giải pháp AI nội bộ hoặc nền tảng "Make in Vietnam" có cam kết bảo mật.*

- **Cấp độ 3 (Dữ liệu cá nhân):** Thông tin định danh hoặc gắn với một cá nhân cụ thể (họ tên, ngày sinh, số CCCD, tình trạng sức khỏe, quan điểm chính trị...). *Phải tuân thủ nghiêm ngặt Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân. Tuyệt đối không đưa lên AI công cộng nếu chưa có sự đồng ý của chủ thể và các biện pháp bảo vệ cần thiết.*

- **Cấp độ 4 (Bí mật nhà nước):** Thông tin thuộc danh mục bí mật nhà nước theo quy định của pháp luật. **Tuyệt đối cấm** đưa vào bất kỳ hệ thống AI nào không được cơ quan có thẩm quyền cấp phép riêng cho việc xử lý tài liệu mật.

Điều 9. Kiểm soát kết nối và tích hợp hệ thống

1. Nghiêm cấm mọi hình thức tự ý kết nối, tích hợp trái phép các hệ thống thông tin nội bộ, hệ thống cơ sở dữ liệu nghiệp vụ của cơ quan vào các nền tảng AI bên ngoài, đặc biệt là các nền tảng AI công cộng không rõ nguồn gốc.

2. Việc tích hợp (nếu có nhu cầu nghiệp vụ) chỉ được thực hiện khi có phê duyệt của cấp có thẩm quyền, sau khi đã được bộ phận chuyên trách (CNTT, an ninh mạng) tiến hành đánh giá rủi ro an ninh mạng chi tiết, có phương án kỹ thuật bảo vệ và phải ghi nhật ký (log) hệ thống đầy đủ để phục vụ công tác giám sát, kiểm tra.

Điều 10. Nhận diện và phòng tránh các rủi ro từ AI tạo sinh

1. **Hiện tượng "Ảo giác" (Hallucination):** Là tình trạng AI tự bịa đặt thông tin, dữ kiện, số liệu hoặc thậm chí là các vụ việc không có thật nhưng trình bày một cách rất logic và thuyết phục. Đây là một trong những rủi ro lớn nhất, đòi hỏi người dùng phải luôn thực hiện quy trình kiểm chứng.

2. **Nội dung giả mạo (Deepfake):** AI có thể được sử dụng để tạo ra các video,

hình ảnh, âm thanh giả mạo. Cần nâng cao cảnh giác, luôn xác thực thông tin từ nhiều kênh chính thức trước khi tin và phổ biến.

3. Tấn công lừa đảo (Phishing) tinh vi: Kẻ xấu có thể dùng AI để soạn các email, tin nhắn lừa đảo với ngôn ngữ tự nhiên, không sai lỗi chính tả, mạo danh đồng nghiệp, cấp trên để yêu cầu chuyển tiền, cung cấp mật khẩu hoặc thông tin nhạy cảm. Cần hết sức cẩn trọng với các yêu cầu đột xuất, bất thường.

4. Lộ lọt thông tin nhạy cảm: Mọi dữ liệu được nhập vào các mô hình AI công cộng đều có thể được nhà cung cấp dịch vụ sử dụng để huấn luyện lại mô hình và có nguy cơ bị truy cập bởi bên thứ ba. Cần ghi nhớ quy tắc vàng: "Đừng nhập vào AI những gì bạn không muốn đăng lên mạng xã hội".

Điều 11. Nhận diện sản phẩm giả mạo (Deepfake)

Cán bộ, công chức cần cảnh giác trước các cuộc gọi video hoặc tin nhắn đa phương tiện có dấu hiệu sau:

- Thời lượng ngắn bất thường, chất lượng kết nối chập chờn (cố tình).
- Khuôn mặt thiếu cảm xúc tự nhiên, mắt ít chớp hoặc hướng nhìn không tập trung.
- Màu sắc da và ánh sáng không khớp với bối cảnh phía sau; vùng cổ hoặc viền tóc bị mờ nhòe.
- Âm thanh giọng nói đều đều, thiếu ngữ điệu tự nhiên hoặc khẩu hình miệng không khớp với lời nói.
- Biện pháp xử lý: Chủ động ngắt cuộc gọi và xác thực lại qua kênh liên lạc truyền thống (điện thoại) trước khi thực hiện bất kỳ giao dịch tài chính hay cung cấp thông tin nào.

CHƯƠNG V GIÁM SÁT, ĐÁNH GIÁ VÀ XỬ LÝ VI PHẠM

Điều 12. Giám sát và đánh giá việc sử dụng AI

1. Việc sử dụng AI được đưa vào nội dung kiểm tra, giám sát thường xuyên và định kỳ của cấp ủy, ủy ban kiểm tra các cấp.
2. Khuyến khích các đơn vị xây dựng sổ theo dõi, nhật ký hoặc báo cáo ngắn gọn về các ứng dụng AI tiêu biểu đã triển khai.
3. Kết quả ứng dụng AI là một tiêu chí tham khảo trong đánh giá mức độ đổi mới, cải cách hành chính và chuyển đổi số của cơ quan, đơn vị.

Điều 13. Xử lý vi phạm

1. Cá nhân, tập thể vi phạm Quy chế này, tùy theo tính chất, mức độ, hậu quả sẽ bị nhắc nhở, phê bình, xử lý kỷ luật theo quy định của Đảng và pháp luật của Nhà nước.

2. Trường hợp vi phạm gây lộ lọt bí mật nhà nước, dữ liệu cá nhân hoặc thiệt hại nghiêm trọng về kinh tế, uy tín thì chuyển cơ quan có thẩm quyền xem xét, xử lý theo quy định pháp luật.

3. Người đứng đầu cơ quan, đơn vị chịu trách nhiệm liên đới nếu để xảy ra vi phạm nghiêm trọng, kéo dài mà không có biện pháp ngăn chặn, xử lý kịp thời.

CHƯƠNG VI TỔ CHỨC THỰC HIỆN

Điều 14. Trách nhiệm của Người đứng đầu các cơ quan, đơn vị, tổ chức đảng

1. Lãnh đạo, chỉ đạo và chịu trách nhiệm toàn diện về việc tổ chức thực hiện quy chế này.

2. Theo dõi, quản lý, giám sát việc sử dụng AI đối với cá nhân thuộc đơn vị mình.

3. Cập nhật, cung cấp danh sách tài khoản, quyền truy cập của cán bộ, đảng viên khi được điều chuyển công tác, nghỉ hưu hoặc nghỉ việc và thông báo bằng văn bản cho bộ phận phụ trách quản lý tài khoản thực thi quy trình thu hồi, khoá hoặc huỷ tài khoản.

Điều 15. Trách nhiệm của công tác giám sát việc khai thác, sử dụng AI

1. Công tác giám sát việc khai thác, sử dụng AI đặt dưới sự lãnh đạo trực tiếp, toàn diện của cấp ủy đảng các cấp; bảo đảm tuân thủ đúng chủ trương, quy định của Đảng, pháp luật của Nhà nước và Quy chế này.

2. Nội dung giám sát tập trung vào: mục đích sử dụng AI; loại hình công cụ AI được sử dụng; mức độ tuân thủ quy định về bảo mật, bảo vệ dữ liệu cá nhân; trách nhiệm kiểm chứng, thẩm định của cá nhân, đơn vị khi sử dụng sản phẩm do AI hỗ trợ.

3. Ủy ban Kiểm tra Đảng ủy phường chủ trì, phối hợp với các bộ phận liên quan thực hiện giám sát chuyên đề hoặc lồng ghép trong các cuộc kiểm tra, giám sát thường xuyên đối với tổ chức đảng, cán bộ, đảng viên trong việc sử dụng AI.

4. Người đứng đầu cơ quan, đơn vị chịu trách nhiệm tổ chức tự kiểm tra, tự giám sát việc sử dụng AI trong phạm vi quản lý; kịp thời nhắc nhở, uốn nắn các biểu hiện sử dụng AI không đúng quy định, có nguy cơ mất an toàn thông tin.

5. Khuyến khích thực hiện giám sát thông qua phản ánh, kiến nghị của cán bộ, đảng viên; bảo đảm nguyên tắc khách quan, công khai, không gây cản trở hoạt động chuyên môn chính đáng.

Điều 16. Trách nhiệm của Văn phòng Đảng ủy

1. Phối hợp với các cơ quan, đơn vị chịu trách nhiệm thực thi quy trình thu hồi, khóa hoặc huỷ tài khoản trong phạm vi quản lý (bao gồm tài khoản AI nội bộ và các tài khoản do cơ quan cấp phép) ngay khi cán bộ, đảng viên điều chuyển công tác,

ngỉ hưu hoặc nghỉ việc.

2. Phối hợp với các cơ quan, đơn vị kịp thời phát hiện nguy cơ mất an toàn thông tin, rủi ro vi phạm để tham mưu cấp có thẩm quyền biện pháp chấn chỉnh, khắc phục.

Điều 17. Trách nhiệm của cán bộ, đảng viên

1. Trách nhiệm giải trình: Phải có khả năng giải trình được quá trình sử dụng AI và cách thức kiểm chứng thông tin khi được yêu cầu.

2. Quản lý tài khoản: Tuân thủ nghiêm ngặt quy định về quản lý tài khoản và mật khẩu. Tuyệt đối không sử dụng email công vụ để đăng ký các dịch vụ AI cá nhân, các nền tảng không được cơ quan cấp phép. Tuyệt đối không đặt mật khẩu tài khoản AI công cộng (hoặc các dịch vụ cá nhân khác) trùng hoặc tương tự với mật khẩu các hệ thống công vụ (email, hệ thống nội bộ). Phải sử dụng mật khẩu mạnh, có tính phức tạp và thực hiện thay đổi định kỳ theo quy chế của cơ quan.

3. Minh bạch (khi cần thiết): Trong các tài liệu lưu hành nội bộ, có thể ghi chú "Nội dung có tham khảo, hỗ trợ từ công cụ AI và đã được kiểm chứng" để tăng tính minh bạch và hình thành ý thức chung trong cơ quan, đơn vị.

Điều 18. Tổ chức thực hiện

1. Các bộ phận, cá nhân tại Điều 2 chịu trách nhiệm thực hiện Quy chế này.

2. Lãnh đạo các cơ quan, đơn vị có trách nhiệm quán triệt và chỉ đạo việc thực hiện Quy chế này trong phạm vi quản lý.

3. Trong quá trình thực hiện, nếu cần sửa đổi, bổ sung để phù hợp với tiến độ công nghệ và yêu cầu thực tiễn công tác, kịp thời phản ánh về Ban Thường vụ Đảng uỷ (thông qua Văn phòng Đảng uỷ) để tổng hợp, trình Ban Thường vụ xem xét, quyết định.

4. Quy chế có hiệu lực kể từ ngày ký.

Nơi nhận:

- TTĐU,
- HĐND, UBND phường,
- UBMTTQ và các tổ chức CT-XH phường,
- BXĐĐ, UBKT, VPĐU,
- Chi, Đảng bộ cơ sở trực thuộc,
- CP.VPĐU,
- Lưu VPĐU.

**T/M BAN THƯỜNG VỤ
BÍ THƯ**

Huỳnh Thị Thùy Trang