



MOXII
AFRICA

GUIDELINES FOR POLITICAL PARTIES & INDEPENDENT CANDIDATES USING GENERATIVE AI

MOXII AFRICA | OCTOBER 2026

CONTENTS

OVERVIEW	3
CORE PRINCIPLES	4
1. Alignment with the Code	4
2. Transparency	4
3. Human oversight	5
4. Privacy and confidentiality	5
5. Ensuring equality and non-discrimination	6
6. Training and literacy	7
7. Responding responsibly	7
PRACTICAL TIPS	9
TAKING IT FORWARD	9



OVERVIEW

In 2024, we published [Guidelines for Political Parties Using Generative AI](#). Since then, people have increasingly made use generative artificial intelligence systems (“GenAI”) to create and share information. As of 2026, thousands of GenAI systems have been created either as self-standing models or as models embedded in different applications, including social media platforms. The widespread use of GenAI has similarly extended to political messaging and campaigning. In the lead-up to the 2026 local government elections, the Independent Electoral Commission (“IEC”) has [warned](#) that 2026 polls are likely to see a shift from broad national misinformation to ward-specific deceptions driven by generative AI tools.

In response, the IEC published the [Electoral Code of Conduct Countering Disinformation](#) in the Local Government Elections (“the Code”). The Code aims to safeguard information integrity by tackling disinformation in election-related communications, conduct, and campaigning, both online and offline. It is binding on all political parties and candidates, and on anyone acting on their behalf, and covers both paid and unpaid content. Recognising that social media and AI can spread misleading content quickly, the Code also sets standards for the use of GenAI. It requires AI-generated (“synthetic”) content to be labelled, and prohibits deceptive synthetic content, as well as fake accounts and automated bots used to mislead or manipulate voters.

- Drawing from Code and building on our 2024 Guidelines, these revised guidelines **set out good practices that political parties and candidates should follow when deploying AI and show how to turn them into their own AI policies**. These guidelines support the Code but do not replace it and are not legal advice. Political parties and candidates should read the Code in full.

GenAI, synthetic content, & electoral integrity



GenAI is generally [understood](#) as a type of artificial intelligence that creates new content, or changes existing content, such as text, images, audio, and video, in response to a prompt. A prompt is simply an instruction or question given to the tool.



Content made by GenAI can be referred to as **synthetic content**. The Code [defines](#) it as audio, image, video, or text generated through the use of AI.



GenAI can be helpful, but it can also be used to create realistic fake images, audio, and video, as well as text that sounds persuasive but is not true. In elections, access to accurate information is critical, so political parties and candidates need to use GenAI responsibly to safeguard [information integrity](#) and [electoral integrity](#).



CORE PRINCIPLES



1. Alignment with the Code

Commitment to and implementation of the Code is non-negotiable.

Parties and candidates **must comply with the Code**, and their **AI policies and practices** must align with it. The Code is binding from the date of its publication until the election results are declared.

WHAT DOES THE CODE SAY?

Section 6 of the Code requires every party and candidate to:

- ✓ Uphold and comply with the Code in good faith, and take all reasonable measures to meet its terms;
- ✓ Check that information shared by them, or on their behalf, is reliable and accurate before it is disseminated;
- ✓ Refrain from running disinformation campaigns, and from producing, spreading, sponsoring, or encouraging information they know is false or have no reasonable grounds to believe is true;
- ✓ Publicly retract and correct disinformation as soon as reasonably practicable, and within 36 hours of becoming aware of it;
- ✓ Raise awareness of the Code and promote compliance among office-bearers, representatives, members, and supporters; and
- ✓ Contribute positively to electoral integrity and cooperate fully with the IEC and other electoral stakeholders.

In practice, this means building these commitments into the party's or candidate's AI policy, and making sure that day-to-day practice, including the work of third parties, matches what the Code requires.



2. Transparency

Transparency is essential to fostering public trust.

Parties and candidates **should disclose**, in as much detail as possible, their use of AI including:

- Which AI tools they use, and what they use them for;
- Where AI is used to generate photorealistic images and/or videos or when it is used to narrate content;
- Whether and how chatbots or automated tools interact with voters;
- Their use of AI in internal processes (i.e. outside of public-facing campaigning);
- What their AI policy covers.

WHAT DOES THE CODE SAY?

Section 9 of the Code requires parties and candidates to **maintain transparency, diligence, and accountability in all communications** disseminated by them or on their behalf.

Although Section 9 does not mention GenAI, it applies to AI-generated content as it does to any other communication.

Section 12 requires that before distribution, every party and candidate must ensure that:

- ✓ All political advertising, including adverts shared on online platforms, is clearly **labelled** with the party or candidate responsible; and
- ✓ Any AI-generated content is clearly **marked** as “synthetic content”.



3. Human oversight

Human oversight is crucial. Always check content before voters see it.

GenAI can make mistakes, invent facts, and be misused. Human oversight is required to check what it produces before voters see it. Parties and candidates should:

- Assign sufficient capacity and training to ensure adequate human oversight;
- Specify who is responsible for overseeing the different GenAI systems being used; and
- Not allow GenAI to post content or message voters without human approval.

WHAT DOES THE CODE SAY?

Accuracy and oversight are required:

- ✓ Section 6(b) requires every party and candidate to ensure that information disseminated by them, or on their behalf, is **checked for accuracy** before it goes out.
- ✓ Section 8(c) requires them to **exercise oversight** over communications and platforms under their direct control and supervision.

These duties apply to GenAI content as they do to any other communication.



4. Privacy and confidentiality

Respect Privacy. Handle voters' data with care.

Parties and candidates must comply with the Protection of Personal Information Act, 2013 (“[POPIA](#)”) when they handle personal information, including when they enter it into GenAI tools.

Many AI tools store what is entered into them, and some use it to train their models, so entering personal information can put it beyond the party's or candidate's control.

They should therefore take care before giving personal or sensitive information to third-party AI tools and only do so where there is a lawful basis and appropriate safeguards are in place.

WHAT DOES THE CODE SAY?

Section 5(d) acknowledges that **protecting voters' personal information is essential to maintaining public trust and upholding free, fair, and credible elections.**

This requires:

- In terms of section 10 (a) and (b) not using, encouraging, or sponsoring tools that spread disinformation or manipulate political discourse or the electorate, including:
 - falsified, fabricated, doxed, or **stolen data** or material; and
 - **targeted advertising, micro-targeting, or targeted falsehoods based on confidential or sensitive personal information** or inherent characteristics, as contemplated under POPIA.
- In terms of section 11(e) parties and candidates must put appropriate and effective measures in place to **safeguard personal information** in their possession or control from unlawful or unauthorised use or access through a data breach.



5. Ensuring equality and non-discrimination

GenAI should be used for good and should do no harm.

AI tools learn from data that may contain bias. As a result, they may stereotype groups, leave people out, or misinterpret context and intention when translating into different languages.

Biased content may lead to harassment, hate speech, or discrimination. Parties and candidates should therefore check what AI produces and test the tools they use. In practice, they should:

- Check AI-generated text, images, and audio for stereotypes and for content that could cause harm;
- Have translations into local languages reviewed by a fluent speaker;
- Choose, where possible, tools that perform well in local languages and contexts;
- Find out how the tools they use were developed and tested, and watch for harmful or unfair results before, during, and after use; and
- Be aware that what they enter into a tool may be used to train it, and avoid entering content that could reinforce bias and harm.

WHAT DOES THE CODE SAY?

Section 7(c) of the Code requires that parties and candidates **do not produce, disseminate, sponsor or encourage** the dissemination of any information or content that may reasonably give rise to **voter dissuasion, public violence, harassment, hate speech or discrimination**

based on a prohibited ground contemplated in section 1 of the Promotion of Equality and Prevention of Unfair Discrimination Act, 2000 (“[PEPUDA](#)”).



6. Training and literacy

Upskilling is essential for the responsible use of GenAI.

Regular training and literacy are important in deploying AI systems in a manner that ensures that information integrity is safeguarded. To make the most of this technology, and to understand how to use it responsibly, it is useful for parties and candidates to explicitly plan for how they can educate their members, especially those who handle public communications, to use AI responsibly and in line with the Code. Training should cover:

- Understanding the Code;
- Understanding internal policies and procedures;
- Knowing how to exercise human oversight;
- Knowing which tools are permissible;
- Knowing what can and can't be shared with GenAI;
- Learning how to recognise deepfakes, cloned voices, and AI-generated text;
- Understanding what to look for, and who to ask when unsure; and
- Knowing who to contact, and what to do, when something goes wrong.

WHAT DOES THE CODE SAY?

The Code focuses on upskilling both internally and externally:

- Section 8(b) requires every party and candidate to encourage their office-bearers, representatives, members, and supporters to **comply with the Code**, and to give them **support and training** in understanding and applying it.
- Section 14(d) requires they also undertake to support the IEC's work to counter disinformation, including by **promoting media and information literacy**, voter education, and multi-stakeholder engagements.



7. Responding responsibly

Things can go wrong. It is necessary to know how to respond swiftly and responsibly.

AI-generated content can look convincing and spread fast. Parties and candidates should know in advance who is responsible for responding, and what happens in various scenarios. Parties and candidates should also understand what consequences may arise from their non-compliance with the Code and what steps they may need to take to rectify this non-compliance.

Where AI-generated content is **mistakenly published** and turns out to be false, misleading, biased, or missing a required label, parties and candidates should:

- Withdraw or correct it publicly as soon as they become aware of it;
- Add the label if one was missing;
- Switch off any chatbot that has given voters wrong information, and correct what it said; and
- Find out how it happened and update internal policies and procedures as necessary.

Where someone else has **produced a fake about a party or candidate**, such as a deepfake or a cloned voice, they should:

- Keep evidence, including links, screenshots, dates, and any original files;
- Report it to [Real411](#); and
- Publish a correction that gives the facts, without reposting the fake content.

Where a member, supporter, agency, or the party or candidate has **used GenAI to share disinformation**, the party or candidate should:

- Retract and correct it publicly, keeping a copy of what was posted before it comes down;
- Publicly reprimand whoever is responsible, and take appropriate action against any member or candidate who is in breach of the Code;
- Report it to Real411;
- Cooperate fully with any investigation; and
- Review what went wrong and how to prevent it happening again.

WHAT DOES THE CODE SAY?

The Code details various reporting and response requirements for parties and candidates. While it doesn't expressly mention GenAI, they apply to AI-generated content as they do to any other content:

- Sections 6(d) and 8(d) require they **publicly retract** and **correct** disinformation or other false and misleading information spread by them or on their behalf, as soon as reasonably practicable and within 36 hours of becoming aware of it. Section 6(d) adds that they must **publicly censure** whoever is responsible.
- Section 8(e) provides that where appropriate and within their control, they must **publicly condemn** and **appropriately sanction** any member or nominated candidate who contravenes the Code or the Act.
- Section 12(a) affirms that they **commit to report** all instances of disinformation or suspected disinformation distributed online to Real411 within 36 hours of becoming aware of it.
- Sections 11(b) and 11(c) provide that they must **monitor** their own and associated online platforms, act rapidly to correct and limit the spread of disinformation and keep records of it.
- Sections 14(e) and 15 requires that they must **assist any lawful investigation**, and any breach of the Code is subject to sanction under the Act.



PRACTICAL TIPS

⚡ Proactive steps

- Map how GenAI is used by listing the tools, who uses them, and what for, including volunteers and agencies acting on their behalf, and agree which tools are approved. Set out how GenAI use will be disclosed, who oversees it, how people will be trained.
- Prepare a response kit, including clear steps to take, people responsible, correction templates, and a contact list for the platforms, Real411, the IEC.
- Publish a list of official channels and name the party or candidate's official accounts and websites, so voters can tell what is genuine and impersonation is easier to spot.
- Publicly share the AI policy.
- Secure accounts with strong passwords and two-step verification, and limit who has access.
- Save the original photos, recordings, and footage of key campaign content, so authenticity can be shown if it is challenged.

🔄 Adaptive efforts

- Review policies and practices regularly, including after a mistake, when a new tool is adopted, or when responsibilities change, in order to keep up with technological and practical developments.
- Refresh training as tools, risks, and responsibilities change, and include new members, volunteers, and agencies.
- Keep a simple record of which tools are used, for what, and who approved the output.
- Follow developments in AI risks and good practice and seek advice from technical experts, academics, civil society, and the IEC. This may include forming an advisory group with diverse experts to provide guidance on emerging AI threats, opportunities, and best practices.
- Conduct audits and impact assessments to understand the effects of AI use on constituents and democratic processes.



TAKING IT FORWARD

GenAI can help parties and candidates reach more voters and work more efficiently. It can also cause real harm if it is used maliciously, carelessly, or irresponsibly. The stakes are high in an election. Voters rely on accurate information to make their choices, and the Code recognises the harm that disinformation causes to free, fair, and credible elections.

Parties and candidates should, if they have not already, put policies in place for the responsible use of GenAI and other digital tools. By adopting a **proactive and adaptive approach** to AI governance, parties and candidates can harness the benefits of GenAI while mitigating their risks. However, policies can only be impactful where there is a genuine commitment to the rule of **law, ethical principles, continuous learning, and accountability and transparency**.

Information integrity and electoral integrity depend on the choices parties and candidates make every day.