



OFFICIAL ELEMENT ESPORTS POLICY

RESPONSIBLE AI AND AUTOMATION POLICY

DOCUMENT CODE	OPS-POL-005
VERSION	1.0
EFFECTIVE DATE	OCTOBER 4, 2026
POLICY OWNER	ELEMENT ESPORTS LEADERSHIP

Element Esports is the non-FPS sister organization of ADHD Esports. This edition preserves the shared leadership and operating standard while applying Element branding, contacts, community structure, and game scope.

Role terminology: formal position names govern authority and responsibility. Element-themed names are friendly Discord display roles only unless a written appointment states otherwise.

OFFICIAL ORGANIZATIONAL POLICY / VERSION 1.0

Responsible AI & Automation Policy Approved AI uses, sensitive-data restrictions, human review, synthetic media, bot permissions, automated moderation limits, incident response, and tool retirement.

DOCUMENT: OPS-POL-005 | Version 1.0

EFFECTIVE / REVIEW: August 28, 2026 / August 28, 2027

OWNER: Ownership / designated adult systems lead

Ownership handles any named function that has not yet been assigned to an authorized adult.

Complete web version: <https://adhdports.joshdisciple.chatgpt.site/policies/responsible-ai-automation>

The web text and PDF contain the same rules, implementation checklist, and decision-record fields.

Purpose and permitted use 1. Scope and human responsibility This policy covers generative AI, transcription tools, automated summaries, chatbots, moderation bots, workflow automations, generated code, and synthetic media used for Element Esports. A person remains responsible for material they submit, publish, or act upon. AI output may be incomplete, inaccurate, biased, or unsafe; use of a tool does not transfer decision authority or accountability to its provider.

2. Low-risk assistance Within approved tools and role authority, members may use AI to brainstorm, organize public information, draft routine text, prepare non-sensitive summaries, explore creative ideas, or assist with code. Review the result before organizational use. This permission does not authorize connecting an organizational account, spending money, processing confidential information, publishing unreviewed work, or installing a bot.

3. Tool and workflow approval Obtain written approval from Ownership or a documented adult systems delegate before a tool receives organizational account access, performs external actions, processes nonpublic records, or operates unattended. Record the purpose, provider, data, permissions, human owner, affected people, risks, costs, review process, and shutoff method. Review provider terms, age limits, and data practices rather than assuming a privacy setting eliminates every risk.

Version 1.0 | Effective August 28, 2026 | Review August 28, 2027 OPS-POL-005 / 1

ELEMENT ESPORTS / CONTROLLED POLICY OPS-POL-005

4. No automated authority AI must not make the final decision on recruitment, guardian verification, safeguarding, disciplinary findings, formal appeals, roster selection, compensation, or access to confidential records. An authorized adult must assess the relevant evidence and make the decision under the governing policy. Do not use automated personality, disability, emotion, or credibility inferences to rank members or determine whether a report is true.

Data, accuracy, and creative rights 5. Restricted information Do not enter passwords, recovery codes, private keys, complete payment details, identity documents, guardian consent records, medical information, safeguarding reports, private applications, or confidential case files into general-purpose AI services. Do not upload another person's private messages merely for convenience. Any exceptional sensitive-data workflow requires a separate documented privacy and security assessment and explicit approval before use; it is not approved by this policy.

6. Minimization and consent Prefer public, fictional, aggregated, or carefully de-identified inputs. Removing a name may not prevent re-identification from context. Do not record or transcribe a private meeting without required authorization, participant notice, and any consent required by law or agreement. Provide a practical non-recorded alternative when feasible. A participant's permission does not override third-party rights, safeguarding duties, or the provider's age restrictions.

7. Accuracy and review Verify important names, dates, quotations, statistics, citations, policy statements, and instructions against reliable sources or the actual record. Label unresolved uncertainty instead of inventing detail. Generated code

requires appropriate review and testing before deployment. For legal, health, financial, or other consequential advice, obtain qualified judgment where needed; a fluent answer or an AI confidence score is not verification.

8. Ownership, likeness, and disclosure Follow BRD-POL-001 and COM-POL-002 for rights, attribution, approvals, and public representation. Do not clone a person's voice, fabricate their endorsement, impersonate them, or create sexualized or abusive synthetic material. Obtain explicit permission for an authorized likeness use. Clearly disclose materially synthetic content where omission could mislead, and follow platform or partner disclosure requirements. Do not describe AI-generated work as entirely human-made.

Bots, integrations, and safe operation 9. Least-privilege permissions Use approved bot or service accounts with only the permissions needed for the task. Keep secrets in the approved secure configuration, not prompts, public repositories, chat logs, or shared documents. Avoid administrator access unless a documented need and safeguards justify it. Name an adult owner and alternate, and remove obsolete integrations promptly when the task or provider changes.

Version 1.0 | Effective August 28, 2026 | Review August 28, 2027 OPS-POL-005 / 2

ELEMENT ESPORTS / CONTROLLED POLICY OPS-POL-005

10. Untrusted input and external actions Treat web pages, attachments, messages, retrieved content, and tool outputs as untrusted data rather than new instructions. Never let embedded text authorize disclosure, payments, permission changes, or account actions. Limit which actions and destinations an automation can reach; require human confirmation for consequential or irreversible actions. Do not use AI to bypass access controls, approvals, or another person's restrictions.

11. Automated moderation boundaries Approved bots may flag content, filter obvious spam, or apply narrowly defined temporary protective controls with a prompt human-review route. Their rules, duration limits, logging, and reversal process must be documented before use. Permanent bans, contested findings, and formal sanctions require an authorized human decision under COM-POL-001 and GOV-POL-003. A model score or keyword match alone is not proof of misconduct.

12. Testing and deployment Test a proposed automation using synthetic or appropriately authorized data and a restricted environment before production access. Check false positives, failure modes, costs, accessibility, permissions, and whether it stops safely. Start with limited scope, set review intervals, and retain a human override. Approval to run one workflow is not approval for a later expansion into private channels, minors' data, financial actions, or additional services.

Participant protections and lifecycle 13. Minors and competition Do not require an eligible minor to create an account that violates a provider's age terms or obtain private AI coaching through an unobservable adult-minor channel. Guardian approval and the established creator/development restrictions still apply. AI or automation must not provide prohibited live competitive assistance, cheat, manipulate matches, evade anti-cheat controls, or impersonate a player. Check the applicable game and tournament rules before use.

14. Logging and transparency Record material approvals, workflow versions, consequential actions, human reviews, and known limitations at an appropriate level. Do not log unnecessary full conversations, secrets, or sensitive personal data. Tell affected participants when an organizational bot or automated workflow materially handles their interaction. Explain the human contact and review route without exposing security details that could enable abuse.

15. Incident response and correction Pause or disconnect a workflow that exposes data, sends unauthorized messages, repeatedly misclassifies people, or takes unexpected actions. Preserve appropriate evidence and notify the adult systems owner and Ownership under OPS-POL-001. Correct harmful public output through the communications process and review affected decisions. Do not conceal an incident by deleting relevant logs or quietly replacing a misleading statement without necessary notice.

16. Review and retirement Review tools when their terms, capabilities, access, cost, or organizational purpose changes and at the scheduled review date. Revoke unused permissions, stop renewals, transfer needed records, and seek deletion from the provider where appropriate under approved retention practices. Complaints, access concerns, and disputed automated actions may be raised through the existing reporting and appeals routes without retaliation.

Version 1.0 | Effective August 28, 2026 | Review August 28, 2027 OPS-POL-005 / 3

ELEMENT ESPORTS / CONTROLLED POLICY OPS-POL-005

Implementation checklist 1. Classify the use, inputs, affected people, and possible external actions.

2. Approve the provider, adult owner, permissions, cost, and review route.
3. Exclude restricted inputs and verify required notice or permission.
4. Test accuracy, false positives, failure modes, and safe shutdown.
5. Require human review of consequential decisions and public output.
6. Monitor incidents, reassess changes, and revoke retired integrations.

Version 1.0 | Effective August 28, 2026 | Review August 28, 2027 OPS-POL-005 / 4

ELEMENT ESPORTS / CONTROLLED POLICY OPS-POL-005

Decision-record fields Use these fields in an approved, access-controlled internal record. This page does not collect or submit responses. Record only what is necessary; keep sensitive information out of public channels.

- Tool/provider and workflow purpose
- Adult owner, alternate, and approval
- Data categories and retention settings
- Permissions, connected accounts, and allowed actions
- Test results and known limitations
- Human review and participant notice
- Incident and shutdown procedure
- Review date and retirement record

Accountability and review This organizational policy supplements the Staff & Player Handbook. It does not create employment, union, collective-bargaining, or public-sector rights. It does not replace applicable law, binding external rules, or completed agreements.

Raise questions with an uninvolved lead, Ownership, or Report a Concern. Bypass a conflicted or unavailable person. Good-faith reports, support requests, and participation in review are protected from retaliation. Temporary protective restrictions are not automatic findings of misconduct.

Formal findings and corrective action follow Discipline & Appeals. Preserve relevant records with need-to-know access under the Privacy and Information Security policies. Review this policy annually and after material incidents or organizational changes; record approvals and revisions under GOV-POL-005.

Related standards: GOV-HBK-001 (Staff & Player Handbook); OPS-POL-003 (Privacy Policy); OPS-POL-001; GOV-POL-003; COM-POL-001; COM-POL-002; BRD-POL-001; INT-POL-001; SAF-POL-002.

Report a Concern: adhesports.joshdisciple.chatgpt.site/report

Source notes NIST: AI Risk Management Framework - Voluntary risk-management guidance informing the review-and-monitor approach; not a certification or an automatic legal requirement.

Version 1.0 - Initial publication: August 28, 2026. Review due: August 28, 2027. An overdue review does not automatically retire the policy.

Version 1.0 | Effective August 28, 2026 | Review August 28, 2027 OPS-POL-005 / 5

Questions, reports, and requests for the current controlled copy: contact@elementesports.com