IPRO

WHITEPAPER

E-Collaboration Tools & Rules:

Policies & Best Practices for the Compliant Management of Microsoft Teams, Zoom, Slack & Other Videoconferencing & Meeting Tools

PART 2: Getting to Work on Policy Rules

The ePolicy INSTITUTE™
www.ePolicyInstitute.com

Nancy Flynn
Founder & Executive Director, The ePolicy Institute™
Author, The e-Policy Handbook, The ePolicy Toolkit, Social Media Rules, E-Mail Rules, Blog Rules, Instant Messaging Rules, Writing Effective E-Mail

Published October 2021
Sponsored by IPRO

PREFACE

IPRO and The ePolicy Institute™ have created this three-part whitepaper, **E-Collaboration Tools & Rules: Policies & Best Practices for the Compliant Management of Microsoft Teams, Zoom, Slack, and Other Videoconferencing & Meeting Tools** to help North American employers develop and implement compliant E-Collaboration Policy programs. Professionally written by the policy experts at the ePolicy Institute, **E-Collaboration Tools & Rules** is designed to help executives in all industries and professions—regulated and unregulated, large and small, public and private—minimize electronic risks, manage content and use, maintain records, and maximize legal and regulatory compliance.

This three-part whitepaper provides a review of the risks inherent in real-time collaboration through instant messaging (IM), chat, videoconferencing, and virtual meetings.

Parts 1 and 3 of this whitepaper address:

- Forming an E-Collaboration Policy Team and Conducting an Audit.
- Technology and Education.

We encourage you to download and use this three-part series to help create your own E-Collaboration Policy program.

Contact Nancy@ePolicyInstitute.com

Getting to Work on Policy Rules

Best Practice 1:

Put the Audit to Work: Create E-Collaboration Policy with Acceptable Use Rules

Once your audit (see part 1) is complete, it's time to start writing the organization's clear, comprehensive, compliant E-Collaboration Policy. Give onsite and work-from-home (WFH) employees specific rules governing behavior and use. Feel free to incorporate these best practices-based usage rules into your policy.

1. Compliance with the organization's E-Collaboration Policy is mandatory 24/7/365.
2. All parties working on behalf of or to benefit the organization are required to know, understand, and adhere to E-Collaboration Policy. Those parties are referred to as "employees" in the policy and include onsite staff, WFH employees, officers, directors, executives, full-time workers, part-time staff, supervisors, managers, professionals, and interns.
3. Policy applies whether you are onsite at an organization facility, at home, or elsewhere.
4. Whether you are using company-owned computer resources or your own personal desktop, laptop, tablet, or mobile device, you must adhere to E-Collaboration Policy.
5. E-collaboration platforms may not be used for illegal or unlawful purposes, including but not limited to copyright infringement, obscene/pornographic content, defamation, fraud, plagiarism, harassment, discrimination, or impersonation among other offensive behaviors.
6. In order to ensure the compliant preservation, protection, and production of business records, use only the organization's approved e-collaboration platforms and accounts—not unauthorized personal tools and accounts—for official business communications.
7. Use e-collaboration tools strictly in compliance with the organization's electronic and HR policies and guidelines, including but not limited to E-Collaboration Policy; Records Retention Policy; Litigation Hold Policy; Mobile Device Policy; Email Policy; Social Media Policy; Web Policy; Security Policy; Privacy Policy; Harassment & Discrimination Policy; Diversity & Inclusion Policy; Confidential & Sensitive Information Policy; Code of Conduct; Ethics Rules; Netiquette Rules; Videoconference Dress Code and Virtual Background Guide.
8. Microsoft Teams, Zoom, and Slack are provided for business collaboration and communication. Limit personal use of these platforms to before and after regular business hours, your lunch hour, and other established work breaks.
9. Treat internal (coworkers, managers, supervisors, executives, directors) and external (clients, consumers, prospects, suppliers) parties with respect and civility, in accordance with the organization's Code of Conduct, Ethics Rules, and Netiquette Rules.

10. Take all necessary precautions to prevent unauthorized access to Microsoft Teams and Zoom, in compliance with the organization's Security Policy.

11. Familiarize yourself with and adhere to the organization's Privacy Policy. Keep confidential company data and customers' sensitive information safe from prying eyes. Unless you have management's permission, do not share, discuss, or record confidential business records, private consumer data, or sensitive information protected by regulatory bodies.

12. Avoid (or adjust) videoconferencing if confidentiality is crucial. For instance, if you're conferencing with a healthcare provider and need to keep protected health information (PHI) under wraps, don't use a free videoconferencing service that's available to the public. Trust only an enterprise service or a dedicated healthcare teleconferencing service to keep PHI private.

13. WFH employees must ensure confidential and sensitive conversations and content cannot be overheard or observed by family, friends, roommates, or other unauthorized parties.

14. WFH staff must make sure no one is visible in the background of videoconferences or recorded during meetings. If your home office has a door, shut it.

15. Assume you are being recorded during every videoconference, webinar, chat, IM, and meeting. Recordings are retained and archived as business records and may one day be subpoenaed and used as evidence in litigation and regulatory investigations.

16. Be cautious about sharing your screen. Before sharing slides or other materials, close all documents, emails, browser windows, and other items you don't want participants to see.

17. Do not view, copy, alter, or destroy data, records, software, or electronic communications belonging to the organization or any individual without permission.

18. Do not share account or password information with anyone without authorization from IT.

19. Never open unexpected videoconference invitations or click on links within unsolicited invitations. Malicious parties use email to send phony meeting invitations. Click and you may be on the receiving end of a virus or malware, which can infect the entire organization.

20. To stave off unwanted attendees and zoombombing, don't post meeting IDs in public forums or reuse meeting codes.

21. Adhere to the organization's Videoconference Dress Code and Virtual Background Guide. You may be conferencing from home, but you must keep your appearance and surroundings professional, particularly when communicating with clients, prospects, and decision makers. If you wouldn't say, do, or wear it at an in-person meeting, don't say, do, or wear it virtually.

22. Contact Compliance if you suspect someone has violated E-Collaboration Policy (accidentally or intentionally). We will make every effort to keep your report anonymous.

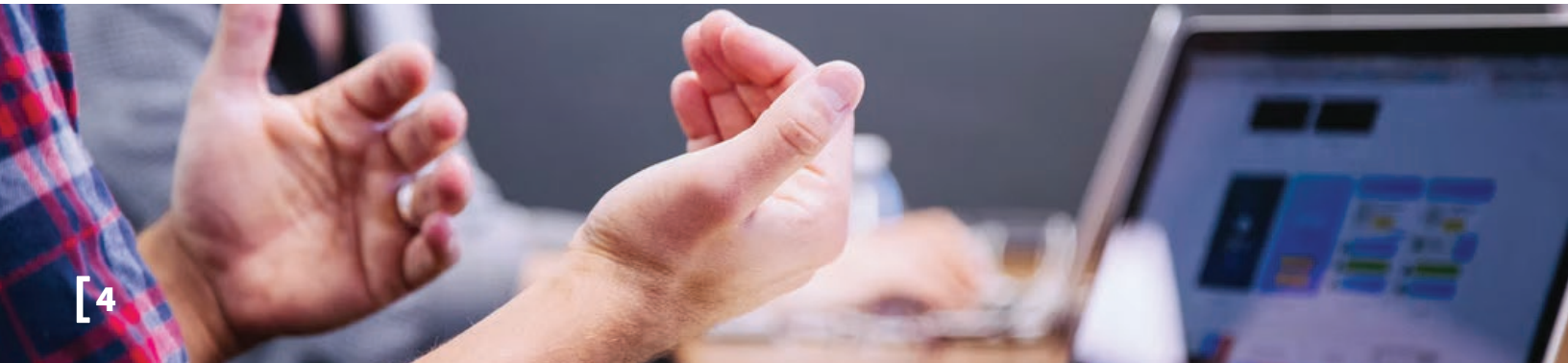
23. Sign and date this E-Collaboration Policy, acknowledging that you have read and understand the policy and will accept the consequences—up to and including employment termination—should you violate policy & procedures.

Best Practice 2:

Use Policy to Spell Out Acceptable Use Rules for Meeting Hosts

In addition to providing employees with usage rules, E-Collaboration Policy should address the special concerns and challenges of meeting hosts.

- Meeting hosts are responsible for ensuring meetings are conducted in a business-professional manner. Only invited individuals may join and participate in meetings. To that end:
    - Password-protect all meetings to block uninvited people (including zoombombers) from attending videoconferences.
    - Assign new ID numbers to each meeting, in order to limit access.
    - Monitor the participant list.
    - Set up a waiting room function.
    - Mute those who are not presenting.
    - Lock the meeting once all expected participants have arrived.
    - Disable participant video if someone is engaging in inappropriate gestures or behavior.
    - Remove disruptive, rude, or otherwise unprofessional individuals from meetings.
- To minimize distractions, Zoom hosts should:
    - Turn off in-meeting file transfer to keep chat free from unsolicited, non-business-related pictures, memes, and content.
    - Disable private chat to prevent participants from messaging one another during meetings.
    - Turn off annotation, so participants can't doodle and write on shared content.
- Inform participants whether they must leave cameras and microphones on for the duration of meetings, or if they are allowed to mute mikes and turn off cameras.
- Let participants know they are being recorded—and explain how the organization plans to use or share the recording. If you are hosting from an all-party consent state or two-party consent state, such as California, permission from all parties is required before recording. Deny meeting access to anyone who does not consent to be recorded.
- Manage screen visibility. Restrict screen sharing to must-see information.
- Establish a separate communications channel to manage screen share and address challenges with co-hosts and presenters—without inadvertently sending a chat to all participants.
- Inform participants when meeting invitations are headed their way. Advance notice will prevent colleagues and clients from clicking on fake invitations from hackers and other bad actors.



Best Practice 3:

Incorporate Content Rules into E-Collaboration Policy

When it comes to Zoom, Slack, and Microsoft Teams, the difference between disaster and compliance often is a matter of content. Racially insensitive, gender-biased, and otherwise offensive or illegal comments can trigger lawsuits and turn off employees, recruits, customers, and the community.

Don't allow users to play fast and loose with language. Incorporate content rules into E-Collaboration Policy to ensure employees support (rather than sink) your commitment to operating an unbiased and respectful culture, free from harassment, discrimination, and incivility.

"More than 40% of Americans have experienced online harassment.[1] In 2020, workers claiming workplace discrimination were awarded over $535 million by the EEOC.[2]"

CONTENT DOs

- Adhere to content rules 24/7/365, at the office and home, using company resources and your own personal accounts and tools.
- Keep business records and other confidential company information under wraps, unless you are approved to share it with authorized parties.
- Maintain respectful interactions with gender-nonbinary people by using gender-neutral pronouns (*they, them, their*) to refer to individuals in all written and verbal business communications. The use of male and female pronouns (*he, she, he/she, he or she*) is prohibited.
- Protect your personal privacy. Never share private information that could harm or embarrass your family, friends, or self.
- Be honest. If you have a vested interested in a topic, say so.
- Write and speak in a conversational, professional tone. In virtual meetings, use the same language you would use during in-person business gatherings.
- Avoid jokes and "funny" text, cartoons, videos, photos, and art. A misguided attempt at humor could prompt a hostile work environment claim.
- Steer clear of content and conversations that could damage the organization's reputation, credibility, or standing with customers, regulators, courts, media, investors, employees, job applicants, government leaders, business decision makers, suppliers, and the general public.
- Adhere to the rules of netiquette, or electronic etiquette. Create content and conduct conversations that are business-appropriate and compliant with regulatory rules and the law.

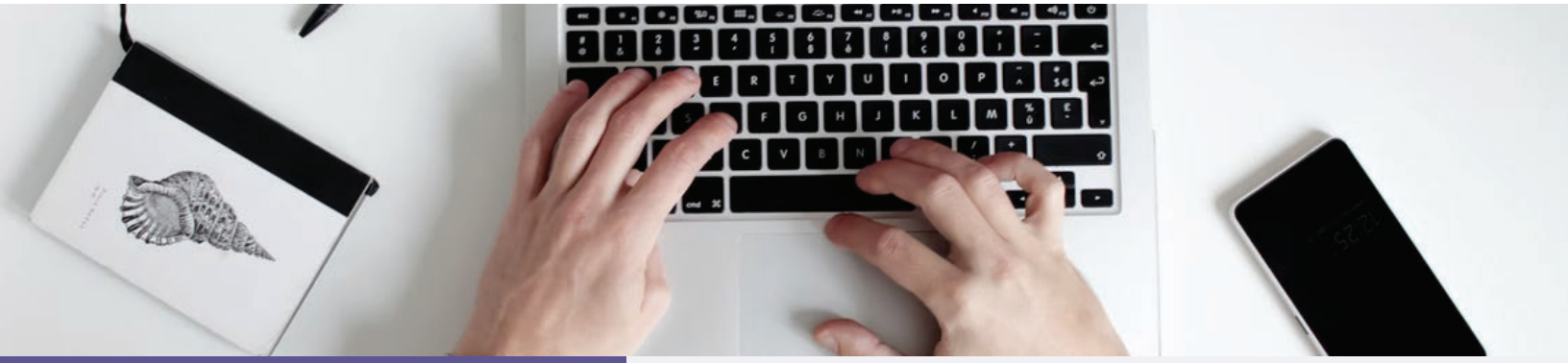
---

1. Pew Research Center, "The State of Online Harassment," January 13, 2021. https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/.

2. U.S. Equal Employment Opportunity Commission, "EEOC Issues Fiscal Year 2020 Agency Financial Report," November 16, 2020. https://www.eeoc.gov/newsroom/eeoc-issues-fiscal-year-2020-agency-financial-report.

CONTENT DON'Ts

- Harass or discriminate against others based on race, color, religion, sex, sexual orientation, sexual identity, national origin, age, disability, ancestry, mental health, veteran status, genetic information, citizenship, or other status protected by law.
- Use language or share content that is fraudulent, harassing, discriminatory, defamatory, obscene, off-color, pornographic, sexually suggestive, profane, abusive, bullying, intimidating, misleading, menacing, offensive, objectionable, inappropriate, unethical, or otherwise prohibited by law or policy.
- Expose/share business records, confidential and sensitive company information, private consumer data, internal email, or other "eyes-only" content that's intended solely for in-house readers.
- Use content/language that is racist, sexist, or discriminatory toward Asian Americans and Pacific Islanders (AAPI), women, Native Americans, Hispanics, Latinos, and other groups. No criticizing, marginalizing, bullying, defaming, or harassing anyone inside or outside the organization.
- Use dismissive, derogatory, or disparaging comments (*OK, Boomer!*) that violate the Federal Age Discrimination in Employment Act (ADEA).
- Gossip or spread rumors about the organization, its customers, employees, or business.
- Whine or complain about personnel, products, programs, practices, policies—or any other aspect of the business.
- Use copyright-protected material without written permission from the copyright holder. No violation of any federal or state laws governing copyrights, trade secrets, patents, proprietary information, or intellectual property among other legal issues.
- Expect privacy when using company resources. Management has the right to access and monitor electronic content on the company system—and personal accounts in some states. All content written, transmitted, accessed, acquired, published, recorded, or stored on the company's system is the property of the organization. Content may be disclosed by management to law enforcement agencies, courts, regulatory bodies, and other third parties without your prior consent.
- Violate content rules and E-Collaboration Policy unless you're prepared to seek employment elsewhere.



Best Practice 4:

Update Records Retention Policy to Cover E-Collaboration Risks

Just like email, the web, and social media, content that is created, shared, transmitted, acquired, recorded, and stored via e-collaboration tools has the potential to create electronic business records. What is an e-business record? Essentially, a business record is the electronic equivalent of DNA evidence—information that may be used to help or hurt the company in litigation. All organizations are obligated to retain business records for their ongoing legal, regulatory, historic, and operational value. If subpoenaed by courts or regulators, business records must be produced promptly and in compliance with the organization's Records Retention Policy and federal/state e-discovery guidelines.

Best Practice 5:

Employ Collaboration-Specific Records Management Strategy

Do not let unmanaged Microsoft Teams, Zoom, Slack, and other e-collaboration content—including recorded chat, IM, videos, webinars, meetings, text transcripts, audio transcripts, and meeting reports—undermine legal and regulatory compliance. Prepare today for tomorrow's e-discovery requests with a collaboration-specific records management strategy:

1. Update Records Retention Policy to address e-collaboration risks and records.

2. Refresh Litigation Hold Policy to halt the destruction of Microsoft Teams, Zoom, Slack, and other e-collaboration records as soon as a regulatory investigation is scheduled, a legal claim is filed, litigation is underway, or a lawsuit is anticipated.

3. Rework your deletion schedule, with e-collaboration in mind. Establish lifecycles for every class of record created, transmitted, acquired, recorded, or stored. Spell out how long records should be retained. Specify when, how, and by whom records may be purged.

4. Rely on best-of-breed third-party technology solutions like IPRO **assess][Hold** and **discovery][Enterprise** to ensure effective retention, archiving, data protection, litigation hold, and e-discovery.

Conclusion: Collaboration Compliance Is as Easy as 1,2,3

To help ensure legal, regulatory, and organizational compliance, adhere to these three steps:

(1) Establish effective E-Collaboration Policy and collaboration-specific Records Retention Policy governing onsite and WFH staff.

(2) Educate employees about risks, rules, records, requirements, and roles.

(3) Enforce policies with disciplinary action supported by IPRO's best-in-class third-party technology solutions. Follow this formula, and you will be well positioned to minimize risks, manage behavior, maintain records, and maximize compliance.

IPRO

The ePolicy INSTITUTE™
www.ePolicyInstitute.com

Seek Competent Legal Counsel

E-Collaboration Tools & Rules: Policies & Best Practices for the Compliant Management of Microsoft Teams, Zoom, Slack, and Other Videoconferencing & Meeting Tools is a general best-practices guide and is intended for informational purposes only. This material is provided with the understanding that neither the ePolicy Institute nor IPRO is rendering legal or regulatory guidance. The author did not and could not contemplate every issue, challenge, or situation that may arise when using e-collaboration tools. Some organizations may be required to comply with different or additional laws, regulations, rules, and procedures from those addressed in this whitepaper. No reliance should be placed on this whitepaper without the advice of experienced legal counsel and other competent professionals including regulatory, records management, IT, security, privacy, and HR experts. Your organization's E-Collaboration Policy (and all electronic policies and procedures for that matter) should be developed with the assistance of a capable attorney.

About The ePolicy Institute

The world's leading e-policy writing, training, and consulting firm, The ePolicy Institute helps employers cut legal and regulatory risks and boost compliance through best practices-based electronic policies and employee training programs. From Alabama to Abu Dhabi, employers rely on the ePolicy Institute to help ensure compliance and reduce risks through the implementation of e-policies governing email, social media, mobile devices, e-collaboration platforms, web, and other electronic business communications tools. An industry pioneer, Founder Nancy Flynn is the author of **The e-Policy Handbook,** the first book to address electronic policies and procedures in the workplace. Her other titles include **The ePolicy Toolkit, The Social Media Handbook,** and **Writing Effective E-Mail.** Trusted for her know-how and integrity, Nancy Flynn is a go-to media source who serves as an expert witness in policy-related litigation. The ePolicy Institute. Keeping you in business and out of court since 1998. Visit **ePolicyInstitute.com** to learn more.

The ePolicy INSTITUTE™
www.ePolicyInstitute.com

IPRO

About IPRO

IPRO is reinventing the way organizations interact with their data. By transforming the electronic discovery reference model (EDRM) and thinking "upstream," we bring insight far earlier in the eDiscovery process, enabling teams inside and outside your organization to collaborate transparently at any stage before data is even collected. By thinking about and interacting with your data differently, you will eliminate waste and reduce risk. We combine best-in-class governance and eDiscovery software with predictive analytics to give corporations, government agencies, law firms, and legal partners the most open and effective solution to data challenges. We bring you this power with an obsession on time-to-value and your success. Visit **IPRO.com** to learn more.

Contact Nancy@ePolicyInstitute.com