SERVING THE PRINTING & GRAPHIC COMMUNICATIONS INDUSTRY IN THE WESTERN U.S.

Native News

pia Services for Graphic Communications

OCTOBER 23, 2023

ISSUE #143

Arizona Par-Tee on the Green Golf Tournament

1st place winners with Cathy Skoglund (Southwest Member Services Director) Kevin Glennen, Marc Graham, and Fernadno Chavez

Our 31st Annual Arizona Par-Tee on the Green Golf Tournament was a huge success! The event took place on September 29 at the Raven Golf Club in Phoenix, Arizona. It was a fabulous day of wonderful weather, great golfing and just plain fun for the 70+ printing industry professionals in attendance.

The event was a success in more ways than one. We are thrilled to announce that $2,973 was raised for the R.A.I.S.E. Foundation through the sale of raffle tickets, mulligan tickets, a 50/50 raffle, and cooler and water sales. The R.A.I.S.E. Foundation supports education in the graphic communications field.

Thank you to everyone who participated in the event as well as our event sponsors, Scottsdale Community College students and everyone else who helped make the Par-Tee on the Green such a success.

Congratulations to our winners:

FIRST PLACE

Prizes: $150 gift cards for Total Wine

Kevin Glennen, Prime Source Printing

Marc Graham, Sun Lakes Pest Control

Matt Fleetwood, Crescent Crown Distributing

Nando Chavez, Crescent Crown Distributing

SECOND PLACE

Prizes: Magnetic Golf Cart Speakers

Paul Mozurkewich, Best Approach

Jerod Wilks, Best Approach

Blanca DiPoce, KellySpicers

David Hardman, Industry Print Solutions

THIRD PLACE

Prizes: $75 gift cards for Top Golf

Brett Wilson, SRP

Andy May

Jim Skoglund, Jimbo's Wing'n It

Scott Downey

COMPETITION HOLES

Prizes: $50 Amazon Gift Cards

Closest in 2 – Jeff Hoffman, KDC Bindery – in the hole!!

Closest to the Pin – Mark Graham, Sun Lakes Pest Control

Men's Long Drive – Brett Wilson, SRP

Women's Long Drive – Tracy Archuleta, Konica Minolta

Longest Putt – Trevis Becker, AlphaGraphics

SPECIAL THANK YOU TO OUR SPONSORS

Kelly Spicers

KYOCERA Document Solutions West

alphagraphics ON UNIVERSITY

XEIKON

HEIDELBERG

MGX

PIASC INSURANCE SERVICES Since 1988

Prudential Overall Supply

O'NEIL MADE TO IMPRESS

FUJIFILM Value from Innovation

KONICA MINOLTA

Canon

MONA POWERED BY NXGEN

KODAK

CREATIVE Document Systems

HR | BIZZ

GPA

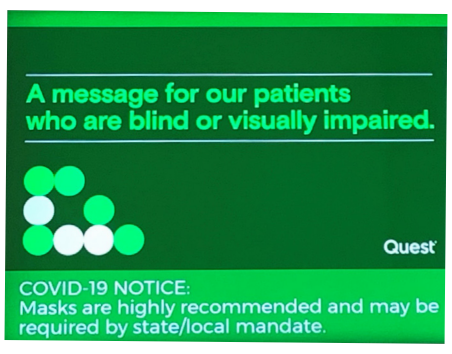
ShieldITNetworks

SCOTTSDALE COMMUNITY COLLEGE A MARICOPA COMMUNITY COLLEGE

BUSINESS MANAGEMENT

Do Your Marketing Tactics Make Sense?

A few months ago I was sitting in the waiting room of my local medical lab waiting to have a routine blood test done. At the front of the room was a large screen on which a rotating loop of images was being shown, primarily ads for the lab company's services.



A message for our patients who are blind or visually impaired.

Quest

COVID-19 NOTICE:
Masks are highly recommended and may be required by state/local mandate.

I thought the image pictured above, along with the image that came after it giving the details of the program, deserved the "Most Poorly Thought Out Marketing Tactic of the Week" Award. How did they expect a blind person sitting in that waiting room to see this silent message that was clearly meant specifically for them?

This marketing tactic simply did not make sense!

Are you thinking through your marketing tactics before implementing them?

Here are some things to avoid…

Nonsensical offers – Is your offer something that your target audience would want, appreciate and/or use? A "buy one get one half price" offer on coffins or king size mattresses is not likely to bring in much extra business. Neither is an offer of same-day delivery of incinerators, which typically require a government permit – and, I'm guessing, a fair amount of planning – to install.

Irrelevant content – If you're going to publish a newsletter or blog, your content needs to be of value to your target audience and relate to what you're selling. Remember, your ultimate goal is to sell. If you're selling financial services to young adults who are at the beginning of their careers, you should be writing about financial services – not office etiquette tips.

Inappropriate locations – Are you advertising/posting/showing up in the places that your target audience is likely to be? For example, if you are marketing to emergency room nurses, you're not likely to meet prospective customers at a meeting for local small business owners.

Shoddy promotional items – Giving away items emblazoned with your logo and contact information can be a great way to stay top of mind. But if these products are shoddy, prospects may think that your offering is shoddy, too.

Irrelevant SEO keywords – When it comes to search engine optimization (SEO), always remember that it doesn't do you any good to be #1 on Google for keywords that your target audience is not likely to use when looking for whatever it is that you're selling. For example, I sell marketing content writing and book ghostwriting services. I don't want to come up as #1 for "graphic design."

Source: Linda Coss, Plumtree Marketing, www.PlumtreeMarketingInc.com

TECHNOLOGY

Making Cyber Security Training Effective

Training employees on anything can be an expensive process. You incur the cost of investing in necessary materials plus the time it takes away from your employees doing revenue-generating activities. But what's worse when it comes to cyber security training is the expense you'll incur if that training fails.

Most employee cyber security training fails

Recent studies show that human error plays a role in a shocking 90% of data breach cases! Smart business owners are taking a proactive approach and training their employees on cyber security do's and don'ts. While we applaud their efforts and encourage all owners to take this step, research suggests their efforts aren't paying off. Despite their willingness to train employees, the number of data breaches continues to increase.

What gives? We'll be the first to say it – cyber security training can be boring. And what happens during boring presentations? People aren't engaged, so they tune out and miss the critical information needed to keep your company secure. After the presentation, they sign off, saying they have learned the lessons. But have they really, or are they a ticking time bomb in your organization?

Try following your training with a phishing simulation

The latter is likely true. If you want the information to stick, you must take some additional steps – and the most important is putting them to the test!

According to Education World, interactive activities are six times more effective when learning and remembering material than simply listening to a lesson. You can incorporate this tactic by putting employees to the test to find out whether or not they can apply what they learned.

One of the best ways to do this is to use phishing simulations. Here's how the process works:

1. **A third party creates a realistic but fake phishing e-mail** that shows identifiable signs discussed in the training. An example could be creating an e-mail that is similar to the CEO's requesting private information, or one that looks like an outside company sending a bad link, etc. You can customize it to look like something relevant that your employees could potentially see and fall for.
2. **The employees are then put to the test.** You choose which employees will receive what links and what dates the e-mails will be sent. Will they be able to identify the threats or will they fall for the scams?
3. **The results are collected and shared with you** to develop more comprehensive training programs and help you identify which employees are your biggest risks, so you can provide specific coaching.

Another great way to use phishing simulations is to send out the tests before the training. When employees see that people in the company are making mistakes, they are more likely to pay attention to the lesson.

It's not enough to just teach the information!

The information must be learned and implemented every day to be effective and keep your organization secure.

If you're looking for effective cyber security awareness training for your employees, our team has a comprehensive program that will engage, teach and test your employees so you can have peace of mind knowing they are working to keep your company safe. To get in touch with our team and get started on your cyber security training session today, visit www.ShieldITNetworks.com/contact-us.

Source: Shield IT Networks, www.ShieldITNetworks.com.

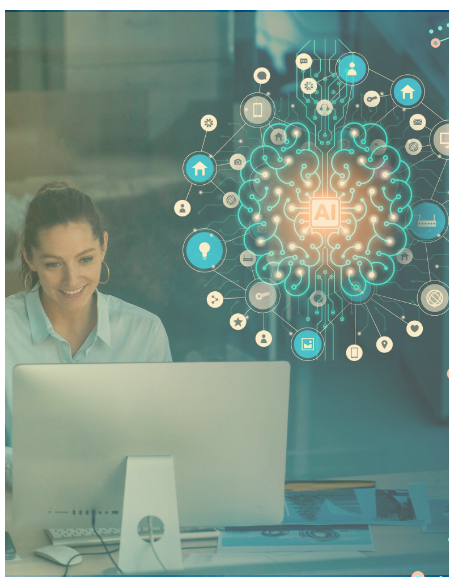
Generative AI is Here – Are Your Workplace Policies Ready?

As generative artificial intelligence (GAI) technology, like ChatGPT, finds new and greater uses in the workplace, employers must consider the myriad of legal and other issues that come with it. For good reason, employers increasingly are implementing policies to mitigate potential risks and ensure safe and permissible uses of GAI by employees. In this post, we highlight key risks and outline strategies for developing policies to mitigate such risks.

What is GAI and how is it being used today?

GAI generally refers to algorithms known as large language models that can be used to create new content, including audio, code, images, text, simulations and videos, based on a user's prompt. GAI models ingest massive data sets of text, information and images from the internet and other sources, which are used to train those models to gradually "learn" and "understand" the relationship between words or data. When a user inputs a prompt, a GAI model generates new text, images or data based on the data set on which it was trained. Some popular GAIs include ChatGPT and Bard (for text generation); DALL-E, Stable Diffusion and Midjourney (for image generation); and Runway and Sythesia (for video generation).

The potential applications and use cases for this powerful technology are numerous, and employees are using these tools to generate software code, draft communications (emails, memos and correspondence), generate ideas and content, outline and summarize lengthy or complex documents, and fact-check existing content. This AI-generated content is then being used in a variety of business operations including marketing, sales, customer support and back-office functions.



What are the risks of employees using GAI at work?

While GAI tools might offer efficiency and shortcuts in generating content, they carry a number of risks that employers need to consider. For example:

- **Inaccuracy/bias:** Text-generating GAI tools produce outputs by predicting the most likely next set of words based on the corpus of data used to train the model. While these tools often provide clear, coherent outputs that may be very reliable, there is always a risk the outputs are inaccurate or misleading. Indeed, developers of these models have acknowledged that sometimes these systems produce "hallucinations" – inaccurate text that is wholly fabricated. Further, these systems are limited by the data used to train them, which itself may be inaccurate, biased or simply limited in scope. ChatGPT discloses that its "knowledge" is limited by any facts arising after 2021.
- **Ethical/moral hazard:** GAI systems are relatively untested and users may not know what, if any, ethical constraints are placed on the GAI, including potential outputs that reinforce or promulgate biases, stereotypes and prejudices, or ignore social or moral conventions entirely.
- **Privacy:** Information included in the prompts for GAI systems may be used by the developer of the model to further train, refine or improve the model. Indeed, ChatGPT's terms explicitly state that its developer may use these prompts for that very purpose. As a result, including any personal information in prompts may violate privacy laws and policies applicable to that organization.
- **Trade secret security/protection of confidential business information:** Similarly, if any confidential or proprietary business or enterprise information is entered into prompts, that data may be shared with the model developer and loses all security and confidentiality protections.
- **Copyright/ contract claims:** Commercial uses of a third-party GAI tool may subject users to copyright infringement claims, breach of contract claims or other claims arising out of violations of the developer's terms of use, or from the duplication of intellectual property that was used in training data.
- **Copyright enforcement/IP ownership:** There is a risk that content created by GAI cannot be copyrighted unless it involves significant human input.
- **Consumer protection and regulatory compliance:** The FTC and other federal agencies have asserted that if consumers are unaware that they are interacting with an automated process (e.g., bot), rather than a human, that may present potentially unfair or deceptive practices. Further, the federal, state and local legal and regulatory frameworks continue to evolve concerning use of this technology, and some of these laws require preservation of data, auditing for potential bias and transparency or explainability duties.
- **Defamation:** Content created with a GAI tool may be offensive, defamatory or otherwise violate workplace policies.
- **Specialized duties:** Certain organizations operating in highly regulated industries may face additional compliance risks arising from such regulations. For example, attorneys considering the use of these tools should consider applicable rules of professional responsibility and avoid over-reliance on GAI, a problem recently highlighted in a well-reported case.

Takeaways for employers

Employers should adopt policies that leverage human oversight, training and monitoring of GAI in the workplace.

Instituting new workplace policies to keep up with technology is nothing new – policies on personal electronic devices and social media use are now almost universal. Like with these technologies, employers first need to assess what their approach will be to GAI and whether, and to what extent, they will allow employees to use such tools for work, and if so, what parameters will apply to internal or external tools. This will depend heavily on the organization's mission, business and workforce, as different industries carry different risks, as does the different potential uses for GAI (in sales, marketing, human resources, etc.).

After determining how the organization may leverage GAI, employers should make their guidelines clear to employees in a written policy. As with existing technology usage policies, a GAI policy should define GAI, explain its risks and set out clear guardrails on permissible or prohibited use. These policies should include terms to ensure the organization takes the following steps:

- **Identify and inventory** all current and potential uses of GAI tools in the organization. This inventory should be refreshed periodically, possibly as frequently as quarterly or semi-annually.
- **Assess the risks** of the current and planned uses of GAI tools. Some applications may present little risk and thus require little oversight, while other applications (including some of those listed above) may need to be closely monitored or even prohibited. For example, it is certainly advisable to prohibit employees from publishing material generated by GAI without any sort of human review, or from inputting confidential data and trade secrets into a GAI tool that will send that data outside the organization. Maintain a record of the current uses, especially those deemed to be high-risk.
- **Clearly identify** permissible and impermissible applications and use cases. Employers should require employees to clarify with management whether they can use certain tools, and consider maintaining a list of permitted or prohibited tools and uses.
- **Adopt transparency protocols** to ensure that employees and external recipients of GAI outputs understand what content was created with GAI tools. Consider whether additional protocols or tags should be used for internal purposes to clearly designate high, medium and low risk outputs.
- **Train managers and employees** on the risks of GAI tools, and the organization's internal policy parameters around the use of such tools.
- **Continually monitor** emerging applications/ use cases and compliance with the policy. Doing so is critical because this technology is rapidly evolving and being deployed in a number of novel ways.

Further, employers should continually assess (and re-assess) what laws or regulations might apply to their employees' use of GAI tools and how their policy could shape compliance. New legal and regulatory frameworks are emerging across numerous jurisdictions, which merits special attention to ensure compliance in this area.

Source: K.C. Halm, Partner; Jeffrey S. Bosley, Partner; Matt Jedreski, Counsel; Erik Mass, Associate; and Brent Hamilton, Associate. Davis Write Tremaine LLP, www.dwt.com.

CONTACT US

Address

5800 S. Eastern Avenue,
Suite 400
Los Angeles, CA 90040
P.O. Box 910936
Los Angeles, CA 90091
Phone: 323.728.9500
www.piasc.org

Key Contacts

LOU CARON,
PRESIDENT
Ext. 274, lou@piasc.org

JUSTIN BOURG,
COMMERCIAL INSURANCE
Ext. 284, justin@piascins.com

EVIE BAÑAGA,
EMPLOYEE BENEFITS
Ext. 224, evie@pibt.org

KRISTY VILLANUEVA,
MEMBER SERVICES
Ext. 215, kristy@piasc.org

RODNEY BOLTON,
HUMAN RESOURCES
Ext. 218, piasc@hrbizz.com

Native News
pia Services for Graphic Communications
OCTOBER 23, 2023 ISSUE 143

Feature	ARIZONA PAR-TEE ON THE GREEN GOLF TOURNAMENT
Business Management	DO YOUR MARKETING TACTICS MAKE SENSE?
Technology	MAKING CYBER SECURITY TRAINING EFFECTIVE
Risk Management	GENERATIVE AI IS HERE – ARE YOUR WORKPLACE POLICIES READY?

pia Services for Graphic Communications
5800 S. Eastern Ave., #400
Los Angeles, CA 90040

Events CALENDAR

● **2023 Americas Print Awards**
TUESDAY,OCTOBER 24
12:00 PM PT
Live on YouTube
Conta.cc/45UD2A8

● **O.S.T.S. Free Webinar: Planning Your 2024 Safety Program**
MONDAY, DECEMBER 11
10:00 AM PT
conta.cc/451ykPH

● **Krazy Krafts Day for Kids**
SATURDAY, DECEMBER 6, 2023
10:00 AM – 4:00 PM PT
International Printing Museum
Carson, CA
printmuseum.org/kraftsday

10 October

SU	MO	TU	WE	TH	FR	SA
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

FOR FULL LIST OF EVENTS, PLEASE VISIT WWW.PIASC.ORG/EVENTS

● **Ben Franklin's Birthday Celebration**
SATURDAY, JANUARY 20
10:00 AM TO 4:00 PM PT
International Printing Museum
Carson, CA
bit.ly/FranklinsBirthday2024

● **NEW DATE: MARCH 28 Paper and Substrate Show**
THURSDAY, MARCH 28
www.piasc.org/papershow/