



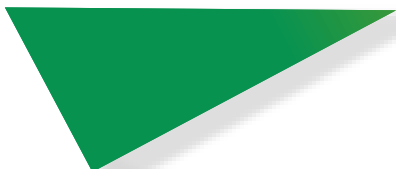
E- Safety Policy

This policy applies to World Green Hub community and all entities affiliated with World Green Hub Ltd. including Aile School
2024-2025

Date of next formal review, Sept 2025

Approved by

Mr. Ahmed Kazzaz, Founder and Director of World Green Hub Ltd.
Dr. Farah Dheyab, Person of Significant Control and Aile School's Founder
Mr. Mohammed Al-Hashimi, Aile School Chairperson of The Governing Body



World Green Hub Philosophy

Unleashing Potential in a Sustainable World...

World Green Hub Ltd. is a learning provider organization deeply integrated with green hubs worldwide, World Green Hub educational philosophy is driven by a commitment to develop responsible, informed, and active Earth stewards, who will lead with empathy, innovate with purpose, and navigate the complexities of life with an unwavering ethical compass. In doing so, World Green Hub serves as a beacon of progressive education for a sustainable and inclusive world.

Vision: A future where education transcends boundaries and transforms lives, driven by the innovative hybrid approach that challenges conventional paradigms, fostering a global community of empowered and socially and environmentally conscious individuals.

Mission: World Green Hub has the mission to forge an educational environment that not only responds to the unique needs of the present and future generations but also empowers students to flourish in a world marked by continual change and innovation.

Belief: World Green Hub centers around the creator and sustainer of the universe. This fundamental belief sets World Green Hub goals and guides its actions, fostering responsibility towards the environment and humanity. It inspires World Green Hub to uphold values of compassion, empathy, and integrity in all aspects of education and community life.

Aim: World Green Hub aims to deliver an extraordinary and enriching educational experience by leveraging technology and artificial intelligence to emulate the education of the future. World Green Hub's vision centers on adaptive learning, empowering students to excel, innovate, and contribute to a more sustainable world.

World Green Hub is committed to provide an adaptive, sustained and quality education that is tailored to individual student needs and nurtures students both intellectually and as global citizens, with a strong emphasis on inclusivity, flexibility, and safeguarding. This e-safety policy seeks to ensure secure, positive, and effective digital learning environment that align with World Green Hub's vision, mission, belief, goals and values.



Introduction

In crafting the ethos of our World Green Hub Community, where technology seamlessly intertwines with the educational journey, we underscore the imperative of conscientiously regulating the use of the internet and technology. This deliberate approach stems from our unwavering commitment to fostering a secure and enriching learning experience for every student. We believe that such measures form the bedrock of our virtual academic community.

We are steadfast in our commitment to empower children as confident, global citizens who utilize the internet and related technologies safely, responsibly, respectfully, and securely. Our approach to virtual education and online safety is designed to be effective, empowering us to both protect and educate individuals on the use of technology, alongside successful learning.

Aim of the Policy:

The goals of applying e-safety policies at World Green Hub is to prioritize student well-being, protect sensitive information, maintain an educational focus, prevent cyber threats, develop responsible digital citizenship, provide parental peace of mind, and ensure legal compliance. These objectives collectively aim to create a secure, positive, and effective digital learning environment for students.

World Green Hub relies on a wide range of technologies to deliver information and offer a high-quality, adaptable, and engaging learning approach. Some of the current internet technologies student might use inside and/or outside of the classroom include:

- **Educational Platforms and Technologies:** Learning Platforms, Virtual Learning Environments, Artificial Intelligence
- **Communication Tools:** E-mail, Instant Messaging, Chat Rooms, Social Networking
- **Digital Content Creation and Sharing:** Cloud Computing (e.g., Google Drive, iCloud Drive, OneDrive), Blogs, Wikis, Podcasting, Video Broadcasting
- **Entertainment and Mobile Devices:** Music Streaming/Downloading, Film/TV Streaming, Gaming, Mobile Devices (e.g., Chromebooks, Laptops, iPads, Tablets), Mobile/Smartphones (with text, video, and web functionality), and other web-enabled mobile devices like Apple Watches.

Our commitment to online safety starts by integrating digital citizenship education into the curriculum to teach students about responsible online behavior, ethical use of technology, and the potential risks associated with online interactions. The curriculum considers age and developmentally appropriate learning material, and the school-wide approaches includes all aspects of school life, including:

- culture
- ethos
- environment
- partnerships with families and the community

Scope:

The entire World Green Hub community and all entities affiliated with World Green Hub Ltd. including Aile School is actively involved in upholding online safety. It is imperative that staff, students, parents and guardians, and affiliated persons collectively promote the agreed-upon principles of online safety. This collaborative effort is essential to effectively manage and mitigate the the 4 C's of the pivotal hazards and risks of uncensored technology:

1. **Content Dynamics:** Tackling the exposure to illicit, inappropriate, or detrimental content, including challenges such as navigating through pornography, counterfeit news, racism, misogyny, self-harm, suicide, antisemitism, and the specter of radicalization and extremism.
2. **Interaction Challenges:** Delving into the realm of potential harm stemming from online exchanges, we address issues like peer pressure, the impact of commercial advertising, and the lurking danger of adults assuming deceptive identities to groom or exploit youngsters for various motives, be it sexual, criminal, financial, or otherwise.
3. **Behavioral Concerns:** A spotlight on personal online conduct that heightens the risk of harm, encompassing actions like creating, sending, or receiving explicit images, both consensual and non-consensual, sharing explicit content, engaging in online bullying, and related behaviors.
4. **Commerce Hazards:** Exploring risks associated with online activities, we navigate the challenges of online gambling, exposure to inappropriate advertising, susceptibility to phishing attempts, and the ever-present threat of financial scams. Our distinctive strategy aims to holistically secure the digital landscape for all users.

Main roles and responsibilities for a safe digital learning environment:

School Members: The engagement with the school's systems begins with the imperative of signing the [Acceptable Use Agreement](#). This commitment extends obligately into off-school time; World Green Hub recognizes that individual virtual behaviour outside platform or school time may impact school or learning virtual environment in all time, non-responsible virtual behaviour increases hazards that may extend to risking safety of the whole school environment and World green Hub platform. However, School actively empowers each individual to engage in meaningful conversations, creating a space where e-safety issues are promptly addressed before causing significant damage, be it during sessions or outside of the school day.

All community members are obligated to network and comminute through World Green Hub platform. World Green Hub or School user account combined with World Green Hub or School user email are the only ones considered safe to use for school purposes, parents and affiliated persons are excluded from this obligation as maintaining safe communication with parents will be through secure access to external school platform.

Senior Management Team: The team takes on a leadership role, actively guiding the implementation of comprehensive e-safety measures, and fostering a culture of continuous improvement to ensure the safety and success of the virtual school's digital environment.

Take the lead in designing and implementing e-safety training programs for staff, educators, and stakeholders, while maintaining open and transparent communication with them to enrich their understanding of e-safety and support them to identify and handle risks promptly by ensuring the availability and accountability of respective staff members to provide support, encouragement, and guidance to parents, students and school community, when needed.

Collaborate closely with the IT department to oversee the implementation and ongoing maintenance of a secure technological infrastructure. This involves aligning technology initiatives with e-safety standards and ensuring regular updates to address emerging threats.

Establish and foster a collaborative network involving all managerial teams to regularly gather feedback, evaluate e-safety policies, and identify areas for improvement. This includes enhancing incident response procedures and planning crisis management strategies to adapt to the evolving digital landscape.

The team ensures whether the school e-safety policy is aligned with e-safety evaluation framework and is consistent with school [policies](#) that have a direct impact on the school safe digital environment, like Privacy, Safeguarding, Anti-Bullying, Anti-Racism, Anti-Discrimination, Behaviour, Wellbeing And Advocacy, Code of Conduct, and Safe and Inclusive Learning Environment policies.

IT Team: The team is responsible for safeguarding school's digital platforms and the data base system, while aligning the digital infrastructure with e-safety standards. They collaborate with senior management team to conduct regular checkups of security awareness for teaching, administrative, and support staff.

The team implements robust measures to monitor internet and email usage with precision, focusing on preventing unauthorized access to school platforms and addressing cyber threats. Data privacy and protection are emphasized through maintaining user authentication confidentiality and monitoring online communications, along with promptly updating software and systems to address security vulnerabilities.

The department actively participates in incident response and reporting, while maintaining digital crisis management drills active and up-to-date. Nevertheless, they maintain continuous collaboration with external cybersecurity agencies to stay informed about the latest threats and best practices, contributing to the resilience of our digital infrastructure.

Welfare Team: The team actively oversees the well-being of both students and staff, ensuring that all school members are considered fairly. They closely collaborate with the school teams to implement e-safety measures and promptly address emerging concerns. The team works in tandem with parents to manage any worries related to student's online activities or cyber threats, providing them with valuable resources and information on online safety.

To foster a safe environment, the team maintain open lines of communication with students, staff, and parents. They also, encourages students to report safety concerns confidentially, fostering a culture where concerns can be reported and addressed promptly.

Additionally, the team collaborates with the school and parents to elevate social engagement standards, contributing to the creation of a positive and welcoming online learning environment.

Academic Team: Coordinators, Subject Leaders, Teachers and Coaches play a pivotal role in ensuring the successful implementation of the Cyber Safety Policy within World Green Hub. Their responsibilities extend to managing and ensuring a safe online classroom environment for all students, this is outlined with the following key responsibilities:

- **E-Safety Education:** Responsible for delivering digital citizenship education as set in the curriculum to equip students with the knowledge and skills necessary for responsible online behavior. Also, integrate e-safety and cyber security topics into regular lessons on a recurring basis, ensuring a consistent emphasis on the importance of cybersecurity, privacy, and ethical online behavior.
- **Positive Online Practices:** Encourage students to follow virtual behavior etiquettes and treat each other with respect and kindness in the digital space. Demonstrate and model safe online practices to set an example for students. This includes using strong passwords, practicing privacy protection, and navigating online platforms responsibly.
- **Communicating with Students:** Ensure ongoing, effective communication with students on e-safety. Cultivate a non-judgmental environment, using age-appropriate language to encourage immediate reporting of any concerns or incidents. A response will be designed accordingly, for example providing clear guidance on seeking advice from appropriate resources.
- **Supervision and Monitoring:** Educators actively monitor and guide online interactions on the student learning platform to ensure respectful communication among students. Promptly address any inappropriate behavior during virtual classes and provide guidance to students on proper online conduct. Vigilant in identifying and evaluating potential e-safety incidents, reporting any concerns to the senior management team.
- **Maintaining E-Safety:** Actively engage in e-safety training programs provided by the school to stay abreast of the latest virtual trends and threats, and apply up-to-date e-safety measures. Collaborate with the IT team and Welfare team to ensure the continuous use of secure online platforms and safe digital learning environment, while maintaining open communication with the Senior Management Team to promptly address any e-safety policy-related issues.
- **Adapting to Changing Technologies:** Stay adaptable and embrace new technologies. Understand the evolving digital landscape to effectively guide students through the challenges and opportunities presented online.
- **Feedback and Continuous Improvement:** Actively participate in the investigation and provide feedback on the effectiveness of e-safety measures, they contribute to the continuous improvement of policies and practices to enhance the overall e-safety framework.

Support Teams: They play a crucial role in implementing e-safety policies, prioritizing them within the broader strategic planning of the school. They don't only apply the e-safety measure, but also provide essential support in the allocation of resources to ensure successful e-safety initiatives, they are on

continuous collaboration with the IT team and Welfare team in maintaining safe virtual school environment, while maintaining open communication with the Senior Management Team to promptly address any e-safety policy-related issues.

For example, the registration team is responsible for authenticating and verifying users during registration, safeguarding sensitive student information, and establishing access controls. They utilize secure communication channels and collaborate closely with IT and administrative teams to maintain a secure technological infrastructure. They actively participate in online safety training, they respond promptly to incidents, ensure compliance with privacy regulations, and communicate securely with academic members. They participate in conducting thorough investigations and implement corrective actions swiftly and effectively in response to e-safety incidents. They also contribute significantly to continuous improvement efforts in online safety measures, reinforcing a proactive and evolving approach within the virtual school community.

For Students: Guidelines for appropriate use of technology, cybersecurity protection, and responsible online behavior:

1. User Authentication and Access Control:

1. Use strong, unique passwords for all accounts.
2. Enable multi-factor authentication when available.
3. Avoid sharing login credentials and never pass password to other students.
4. The school student email is authorized for use exclusively for school purposes.

2. Appropriate Use of Devices:

1. When using personal cyber account or school platforms, use personal devices only.
2. For school purposes, ensure that your speakers, microphone, and webcam are functioning properly to facilitate effective class interaction.
3. Refrain from downloading or installing unauthorized software or apps, and you are advised to download and use school's recommended software or apps.
4. Students are responsible for the proper use of devices, unauthorized access, downloading or sharing of a hazard content, hacking, or any activities that violate local, regional, or cyber laws, is strictly prohibited.
5. Familiarize yourself with basic technology troubleshooting to minimize disruptions during online sessions.

3. Protection Against Cyber Threats:

1. Try to keep all software, antivirus, and security applications up-to-date.
2. Be cautious of phishing attempts and suspicious emails. Verify sources before clicking on links.

3. Don't hesitate to report any cybersecurity concerns or incidents immediately to the IT team.

4. Digital Literacy:

1. Strive to master the concept of digital citizenship.
2. Seek updated information on the safest online behaviour and best cybersecurity practices.
3. Reflect your digital awareness, and consider the consequences of inappropriate cyber behaviour or online activities.
4. When providing feedback or participating in discussions, focus on constructive and positive contributions.
5. When posting or writing an email, make sure to use polite language, keep your message clear and to the point, double-check for any spelling or grammar mistakes, and ensure you are sending it to the correct recipient.

5. Privacy Protection:

1. Understand and respect the privacy settings of others and online platforms.
2. Report any unauthorized access or privacy breaches to the IT team.
3. Avoid sharing personal data, such as addresses, phone numbers, or financial details.
4. Only share personal digital media when approved by your parents or guardians.
5. Always check with a trusted adult before accepting a call from a stranger.
6. Only accept video calls from strangers when approved by your parents or guardians.

6. Social Interaction:

1. Maintain a respectful tone and contribute meaningfully in online discussions, and other communication platforms.
2. Avoid cyberbullying, harassment, or any form of harmful behavior.
3. Think before posting, ensure your content aligns with global community standards and school values, and avoid sharing information that compromises your privacy.

7. Pay Attention:

Do not automatically assume that what you see online is true, valid or acceptable, always judge and consider:

1. whether a website, URL or email is fake
2. what cookies do and what information you are sharing

3. if a person or organization is who they say they are
4. why a person wants you to see, send or believe something
5. why a person wants your personal information
6. the reason why something has been posted
7. whether something you see online is fact or opinion

8. Exercise caution:

1. Refraining from posting or endorsing inappropriate or offensive content, including material of a sexual or discriminatory nature.
2. Avoid access to concerning materials, deliberate access to inappropriate materials will be recorded.
3. Avoid any unauthorized editing or sharing of school digital materials.
4. Refraining from collecting user's information without their permission, or claiming authorship or ownership of a digital work but it actually belongs to others, that would be a form of digital plagiarism or misrepresentation.
5. Refraining from registering or filling any information as or on behalf of anyone else, impersonate anyone else or misrepresent your identity or your age. Be careful not to place or transmit false or misleading information on or through the website.

9. Involve School:

1. Always motivate yourself to report any instances of cyberbullying, harassment, or any behaviour threats your safety or wellbeing while being online.
2. Make sure to inform the school if a school member faces a cyber threat or practice irresponsible digital behaviour, or any concern you might think it will disturb the safety of the school digital space or community.
3. If you have concerns on digital plagiarism or misrepresentation of digital materials, don't hastate to inform the school.

10. Involve Parents:

1. Seek guidance from your parents when there are concerns or situations that you perceive as potential threats to your wellbeing or online safety.
2. Be vigilant and promptly inform your parents if you become aware of anyone, including friends or staff, facing a potential cyber threat or engaging in irresponsible digital behavior.



11. Session Etiquette:

To promote active engagement and participation, and maintain a focused and organized virtual classroom for an effective online learning experience:

1. You are requested to have your webcam and speakers turned on during live class sessions, keep your microphone muted unless instructed otherwise by the teacher, be mindful of background noise.
2. Ensure your face is visible and wear suitable clothes for public appearance when using a webcam, maintain an appropriate and non-distracting background with no one else showing.
3. Use courteous and respectful language in all written and verbal communication, addressing both peers and educators.
4. During live sessions, respond to educator's requests promptly when possible, and demonstrate a commitment to effective communication and collaboration.
5. Before posting comments or questions, review and consider their appropriateness and relevance to the discussion topic.

For Parents:

Parental collaboration is essential for creating a comprehensive approach to online safety. We continually encourage your engagement in your child's online learning and activities. Resources and guidance materials will be provided to enhance your understanding of the technologies used in the learning process and the e-safety principles.

As a parent, you can actively contribute to online safety by following these practices:

- **Enhancing Digital Protection:** It is crucial to implement security measures such as setting strong passwords, using website filters, installing reliable antivirus programs, and setting parental controls. Regularly reviewing and updating these security settings is essential.
- **Addressing Online Safety:** Take proactive steps to address online safety in both home and in the educational setting. Reinforce the lessons taught at school by continuing the conversation about online safety at home.
- **Setting Positive Examples:** You serve as role models for your child. By demonstrating responsible online behavior and adhering to good digital practices, you contribute to shaping positive attitudes towards online safety in the family and community.
- **Monitoring and Supervision:** You are in a prime position to monitor and supervise your child's online activities at home. This includes setting and enforcing rules, managing screen time, and ensuring that children navigate the internet safely. The school, being on the other end, might not have the same level of oversight.
- **Personalized Guidance:** Provide personalized guidance based on your knowledge of your child's behavior, interests, and online activities. This individualized approach enhances the effectiveness of online safety education, addressing specific concerns that may be unique to each child.

- **Observing changes:** If notable changes occur, such as an increased obsession with the internet or a departure from their usual demeanor, it is crucial to initiate a thoughtful conversation. By addressing abnormal behavior promptly, collaboratively can identify the underlying issues and work towards effective solutions.
- **Open Communication:** Foster open communication with your child, encouraging them to share their online experiences, challenges, or concerns. This open dialogue allows for timely intervention and support, creating a supportive network that extends beyond the school environment.
- **Cultivating Digital Awareness:** you are encouraged to instill in your child a sense of caution in the cyber world. This involves educating about the importance of safeguarding personal information, exercising discretion when interacting with strangers online, and being wary of exaggerated claims or promises.
- **Fostering a Culture of Seeking Help:** Teaching children how to seek assistance when faced with cyber threats is pivotal. Whether it's calling you upon encountering a stranger or confiding in a teacher about inappropriate online content, instilling the confidence to ask for help is a fundamental aspect of their digital resilience.
- **Staying Informed:** The online landscape is dynamic and continually evolving. Being actively involved in your child's digital life allows you to stay informed about the latest online trends, apps, and potential risks.
- **Understanding School Policies:** Parental awareness of school policies enhances the effectiveness of such policies. Gain insights into what is being practiced at school to reinforce these practices at home.

By following these practices, you will play a crucial role in creating a safe and secure online environment for your child.

Parental Consent for Student Participation:

In line with World Green Hub's dedication to implementing an adaptive learning approach tailored to each student's unique needs, parents are invited to choose the preferred mode of engagement for their child during online classes. This flexibility ensures that students can participate in a way that best suits their well-being. Students may opt to use the webcam for visual participation during live class sessions, the microphone for verbal interaction when necessary, or participate through written communication, such as chat or discussion forums. Importantly, the choice of any combination of these options should not impact a student's grades or standing in the course rather than fostering an environment conducive to thriving and successful learning experiences.

Students can Join the Network of Green Hubs and participate within Green Hubs activities and events through their parents account. This option is contingent upon obtaining [Parental Agreement](#) and authorizing [Network Terms of Use](#). In addition they are advised to follow "Digital & Social Awareness Guide" which is designed to enhance students' understanding of digital technologies, social media platforms, and their impact on personal and social well-being. The guide covers topics like online

safety, responsible digital citizenship, social media literacy, cybersecurity, privacy concerns, digital well-being, and the impact of digital technology on society.

The inclusion of these criteria ensures that students are equipped with the necessary knowledge and skills for responsible online engagement, while parental consent and supervision serves as an additional layer of safeguarding in alignment with the school's commitment to promoting a secure and positive digital environment.

Media Materials Usage Policy for Publicity: This part governs the use of photos and video recordings for publicity on social media, affiliated entities websites, and World Green Hub related platforms. All media materials featuring World Green Hub members will be used responsibly and with the explicit consent of parents or legal guardians.

- **Parental Agreement:** Prior to using any media materials featuring students, explicit consent will be obtained from parents or legal guardians through [Parental Agreement For Digital Content Use](#).
- **Purpose of Use:** Media materials will only be used for education publicity material related to World Green Hub or affiliated entities, like showcasing achievements, events, year book, and promoting a positive image of our community.
- **Respect for Privacy:** Privacy considerations will be paramount, ensuring that media materials respect the dignity and personal space of individuals.
- **Opt-Out Option:** Parents have the option to opt-out of media coverage for their child by notifying the World Green Hub alongside the affiliated entity in writing.

By adhering to these guidelines, we ensure responsible and respectful use of media materials, fostering a positive online presence for our World Green Hub community.

Reporting Mechanism:

By ensuring clear channels of communication, we aim to promptly define any safety concerns or issues to provide students with the necessary support and guidance to the overall security and well-being of the online learning environment:

- A transparent reporting mechanism is established for students, parents, and staff to report incidents as stated in [‘The Inquiry, Concern and Complaint Policy’](#). Reports are treated with confidentiality, and appropriate actions are taken to address and resolve incidents.
- Teachers serve as the primary point of contact for students to report safety concerns during live sessions. Throughout the school day, the school [Welfare Team](#) and the [IT team](#) is the designated contact for e-safety matters. Outside of school hours, we encourage students to report incidents to their parents first, as we regard parents as the foremost source of guidance and advice, subsequently, parents can contact the school on behalf of the student to deliver concerns regarding school e-safety matters.

- World Green Hub members should contact the [IT Team](#) for a comprehensive range of technical support, including data security concerns, security breaches like unauthorized access or potential cyber threats, inappropriate content including harmful or offensive material encountered online, phishing attempts or suspicious online communication aiming to deceive or compromise personal information, software/application issues, network performance problems, device configuration assistance, and technology training needs.
- [Welfare Team](#) is the point of contact for cyberbullying, mental health concerns, concerns about online relationships, and general well-being and safety. Seeking advice from the Welfare Team is recommended for navigating online challenges, understanding online etiquette and citizenship, and maintaining a healthy balance between online and offline life. This Team helps students efficiently access the appropriate support and guidance based on the nature of their e-safety issue.
- Community members should contact World Green Hub Ltd. [Director](#) in cases involving widespread or systematic violations of e-safety policies, potential legal implications, community-wide concerns, or when issues reported to the IT or welfare teams remain unresolved or escalate.
- Any one is encouraged to deliver her or his concerns regarding e-safety policy measures to the [Senior Leadership Team](#) as a complain. The School or World Green Hub will treat the concern as an emergency issue.
- The Senior Management Team is responsible for maintaining records of incidents and the support provided in their respective assigned areas.

Infringement e-Safety Policies: Violating e-safety policies may result in consequences such as mandatory intervention programs, restricted digital access, parental involvement, and potential disciplinary actions, including suspension or legal consequences for severe violations, as stated in The Code of Conduct Policy. The aim is to educate students, deter inappropriate online behavior.

Contact Information

- World Green Hub Ltd. Director: ahmed.kazzaz@worldgreenhub.com
- Senior Leadership Team: adminstration@worldgreenhub.com
- IT Team: it@worldgreenhub.com
- Welfare Team: support@worldgreenhub.com
- **Emergency: call +447477205461**

Final Statement

In our ongoing dedication to maintaining a safe and secure digital environment, we initiate thorough review of our E-Safety Policy each year. This process is designed to evaluate the policy's effectiveness, relevance, and alignment with the latest technological advancements, educational practices, and legal standards. Your insights and contributions are essential for sufficient review, ensuring that our E-Safety Policy remains a robust and proactive framework for safeguarding the digital well-being of our community.

In conclusion, this policy serves as a foundational framework to ensure a secure and respectful environment for all stakeholders. By adhering to these guidelines, we collectively contribute to fostering a community that prioritizes safety, respect, and responsible conduct. Your commitment to upholding these principles is instrumental in maintaining a positive and inclusive atmosphere within our school

For any questions or further clarification regarding privacy and security of information, please contact World green Hub Ltd. at info@worldgreenhub.com, or call +447477205461.

This policy has been reviewed by The Senior Leadership Team and Aile School's Founder and will take effect as of 7/2/2024.

