Policy Title:	Acceptable Use of Technology Policy

1 Rationale:

Dubai Schools recognize that excellence in education requires that technology is seamlessly integrated throughout the educational program. Increasing access to technology is essential for that future. We also recognize that technology plays an important and positive role in everyone's lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly. This is part of our safeguarding responsibility.

We are also committed to ensuring that all those who work with children and young people, including their parents are informed about the ever-changing risks so that they can take an active part in the safeguarding of children.

The policies, procedures and information within this document apply to all wireless mobile devices used, including any other device considered by the Leadership Team to come under this policy.

2 Aims:

The aims of this policy are to ensure that:

- all users are aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources
- the internet, mobile and digital technologies are used safely, for their intended educational purpose, in ways that will not infringe legal requirements or create unnecessary risk
- students are not knowingly subject to identity theft and therefore fraud
- students avoid cyber-bullying and do not become a victim of abuse or radicalization

3 Policy Statement:

Users of the internet, mobile and digital technologies should do so responsibly and strictly in accordance with the conditions set out in this policy. This policy also includes expectations on appropriate online behavior and use of technology outside of school for students, parents, staff and all other visitors to the school.

BYOD, while not school property, also fall under the Acceptable Use Policy whilst on school property or whilst on school related activities. However, the school is not responsible for the repairs, loss or theft or any damage resulting from their use on school property or during school related activities. Improper use of BYOD will lead to immediate confiscation and permanent denied access to the school Wi-Fi network. The devices will only be returned the parents or legal guardians of the student owning the device.

4 Policy Procedure

Dubai Schools educates students both in the proper use of technology and about the serious consequences of misuse and cyberbullying and will, through curriculum links, computing lessons and assemblies, continue to inform and educate its students in these fast-changing areas. Appendix 1 lists the main risks associated with E-learning and how these risks can be mitigated.

All students and teachers must sign the Acceptable Use of Technology Agreement.

4.1 Email

Staff should use their school email account for all official communication to ensure everyone is protected through the traceability of communication.

Under no circumstances should staff contact pupils, parents or conduct any school business using a personal email address.

Students may only use school approved accounts on the school system and only for educational purposes.

For advice on emailing, sharing personal or confidential information refer to the policy for GDPR.

Emails created or received as part of any school role will be subject to disclosure in response to a request for information.

Staff, and students should not open emails or attachments from suspect sources and should report their receipt to a member of staff immediately.

Users must not send emails which are offensive, embarrassing or upsetting to anyone.

4.2 Visiting online sites and downloading

Staff must preview sites, software and apps before their use in school or before recommending them to students.

Before using any online service that requires user accounts to be created or the sharing of any personal data, staff must consult with the Principal.

If internet research is set for homework, specific sites will be suggested must have previously been checked by the teacher.

All users must observe copyright of materials from electronic sources.

Staff must only use pre-approved systems if creating blogs, wikis or other online areas in order to communicate with students/ families.

Students are not allowed to load extra software/Apps on the school mobile devices. School mobile devices will be synchronized so that they contain the necessary apps for schoolwork. BYOD users may have to install software at home at the family's discretion and expense.

The screensaver or background photo may not be changed for any reason on any school mobile devices. Any changes to the display of the school mobile device will be deemed a violation of this policy.
Inappropriate material or photos are not to be stored on school or BYOD.
BYOD containing material considered inappropriate by the school will be confiscated and returned only to a responsible adult. The device may not be brought to school until the offending material/Apps are removed.

When working with students searching for images, this should be done through Google Safe Search, Google Advanced Search or a similar application that provides greater safety than a standard search engine.

Users must not:

Visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:

- Indecent images of children actually or apparently under the age of 18 or images of child abuse (i.e. images of children, digital or cartoons, involved in sexual activity or posed to be sexually provocative)
- Indecent images of vulnerable people over the age of 18 (i.e. images of vulnerable people, digital or cartoons involved in sexual activity or posed to be sexually provocative)
- Promoting discrimination of any kind in relation to the protected characteristics: gender identity and reassignment, gender/sex, pregnancy and maternity, race, religion, sexual orientation, age and marital status
- Promoting hatred against any individual or group from the protected characteristics above
- Promoting illegal acts including physical or sexual abuse of children or adults, violence, bomb making, drug and alcohol abuse and software piracy
- Any material that may bring the school/Taaleem or any individual within it into disrepute e.g. promotion of violence, gambling, libel and disrespect

Users must not:

- Reveal or publicize confidential or proprietary information
- Intentionally interfere with the normal operation of the internet connection, including the propagation of computer viruses
- Transmit unsolicited commercial or advertising material either to other users, or to organizations connected to other networks except where permission has been given to the school
- Use the school's hardware and Wi-Fi facilities for running a private business
- Intimidate, threaten or cause harm to others
- Access or interfere in any way with other users' accounts
- Use software or hardware that has been prohibited by the school

All breaches of prohibited behaviors detailed above will be investigated, where appropriate, in liaison with the police.

Dubai Schools recognize that in certain planned curricular activities, access to controversial and/or

offensive online content may be beneficial for educational use. In such circumstances, there is an expectation that access is pre-planned, risk assessed and recorded, and permission given by the Principal.

4.3 Storage of Images

Photographs and videos provide valuable evidence of students' achievement and progress in a variety of contexts and can be used to celebrate the work of the school. In line with GDPR they are used only with the written consent of parents which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents at any time.

Photographs and images of students are only stored on the school's agreed secure networks which include some cloud-based services.

Staff and students may have temporary access to photographs taken during a class session, but these will be used solely for learning purposes.

Parents should note that there may be some children who must not have their image put online. For these reasons parents must follow the school's Acceptable Use Agreement and refrain from taking or posting online photographs of any member of the school community, other than their own child/ren.

Staff and other professionals working with students, must only use school equipment to record images of pupils whether on or off site. Permission to use images is sought on joining the school.

4.4 Use of personal mobile devices (including phones)

The school allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in classrooms in the presence of students. Teachers are not permitted to contact a student or parent using their personal device, the only exception would be in the case of an emergency such as a serious accident.

Parents may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities. Under no circumstance should images be taken at any time on school premises or on off-site school events and activities of anyone other than their own child, unless there is a pre-specified permission.

Older students may bring their personal mobile devices/phones to school but must not use them for personal purposes within lesson time. In lesson times all such devices must be switched off unless a teacher has given permission for a devise to be used. Under no circumstance should students use their personal mobile devices/phones to take images of :

- any other pupil unless they and their parents have given agreement in advance
- any member of staff

The school is not responsible for the loss, damage or theft on school premises of any personal devices. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

4.5 New technological devices

New personal technological devices may offer opportunities for teaching and learning. However, the school must consider educational benefit and carry out risk assessment before use in school is allowed. Parents, students and staff should not assume that new technological devices will be allowed in school and should check with the Principal before they are brought into school.

4.6 Reporting incidents, abuse and inappropriate material and inspection of devices

There may be occasions in school when either a student or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the student or adult must report the incident immediately to the first available member of staff, and the Principal. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, refer details to the police.

Students may be selected at random to provide their device for inspection including BYOD to ensure that there are not any violations to this policy.

4.7 Teaching of online safety

Online safety is embedded within the curriculum. The school provides a comprehensive curriculum for online safety which enables pupils to become informed, safe and responsible. This includes teaching to prevent radicalization.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for students to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly.

Students are taught to recognize the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work also includes:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation to enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills in relation to online content e.g. recognizing fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online

pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives)

- Understanding the dangers of giving out personal details online (e.g. full name, address, mobile/home phone numbers, school details, IM/email address) and the importance of maintaining maximum privacy online
- Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversations
- Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images
- What constitutes cyberbullying, how to avoid it, the impact it has and how to access help.

4.8 Care of equipment

General Precautions

- School mobile devices are school property and all users will follow this policy and the acceptable use policy for technology
- Only use a clean, soft cloth to clean the screen, no cleansers of any type.
- Cords and cables must be inserted carefully into the mobile device to prevent damage.
- School mobile devices must remain free of any writing, drawing, stickers, or labels.
- School mobile devices left unsupervised are at the user's own risk.
- For personal devices, parents must ensure their child's mobile device comes to school fully charged and loaded with Apps requested by the school.
- Do not leave the mobile device in an open carry bag so as to prevent it from falling out or from theft
- Students will be held responsible for maintaining their own devices and keeping them in good working order whilst in their possession.
- BYOD devices must be recharged and ready for school each day.
- The school will be responsible for repairing only school owned Mobile devices that malfunction. Mobile devices that have been damaged from student/staff misuse or neglect will be repaired with cost being borne by the student/staff. In the event of an accidental damage, the school on a case to-case basis may exercise discretion in recovering the cost of repair to the device from the user.

Vandalism

Vandalism is defined as any action that harms or damages any equipment or data that is part of the School's ICT facilities. This includes, but is not limited to:

- Deliberate damage to computer hardware such as screen, monitors, base units, printers, keyboards, mouse or other hardware
- Change or removal of software

- Unauthorized configuration changes
- Creation or uploading of computer viruses
- Deliberate deletion of files.

Parents will be immediately notified of vandalism and may be billed for the cost of repair or replacement of equipment.

4.9 Working in Partnership with Parents

Taaleem Partnership Schools work closely with families to help ensure that children can use internet, mobile and digital technologies safely and responsibly both at home and school. It is important that parents understand the crucial role they play in this process. The school seeks to regularly consult and discuss online safety with parents and seeks to promote a wide understanding of the benefits of new technologies and associated risks.

Parents are asked to read, discuss and co-sign with each child the Acceptable Use Agreement. The Acceptable Use Agreement explains the school's expectations and student and parent responsibilities. The support of parents is essential to implement the online safety policy effectively and keep all children safe.

4.10 Records, monitoring and review

Dubai Schools recognize the need to record online safety incidents and to monitor and review policies and procedures regularly in order to ensure they are effective and that the risks to students and staff are minimized.

All breaches of this policy must be reported and all reported incidents will be logged. All staff have the individual responsibility to ensure that incidents have been correctly recorded, acted upon and reported.

The school supports students and staff who have been affected by a policy breach. Where there is inappropriate or illegal use of internet, mobile and digital technologies, this will be dealt with under the school's behavior and disciplinary policies as appropriate. Breaches may also lead to criminal or civil proceedings.

5. Roles & Responsibilities:

Staff:

All staff have a responsibility to ensure that the online safety policy and practice is embedded to prevent misuse of equipment and cyberbullying.

All breaches of this policy must be reported to the Principal.

All breaches of this policy that may have put a child at risk must also be reported to the Designated

Safeguarding Lead.

External organizations who provide extra-curricular activities should have and follow their own online safety policy and acceptable use agreements. However, if the organization has any access to the school network and equipment then they must adhere to the school's online safety procedures and acceptable use agreements. If the organization is operating in school time or when pupils are on site in the care of the school, then the safeguarding of pupils is paramount and the organization must adhere to the school's online safety procedures and acceptable use agreements.

Students have a responsibility to:

- use computers/mobile devices in a responsible and ethical manner.
- Obey general school rules concerning behavior and communication that apply to Technology equipment use.
- Use all technology resources in an appropriate manner so as to not damage school equipment. This "damage" includes, but is not limited to, the loss of data resulting from delays, non-deliveries, mis- deliveries or service interruptions caused by the student's own negligence, errors or omissions. Use of any information obtained via the school's designated Internet System is at your own risk. The school and Taaleem specifically denies any responsibility for the accuracy or quality of information obtained through its services.
- Help the school protect our computer system/device by contacting a teacher about any security problems they may encounter.
- Monitor all activity on their account(s).
- Always turn off and secure the mobile device and BYOD devices after they are done working to protect their work and information.
- Ensure all BYOD/school provided devices are fully charged at the start of the school day.
- Ensure their BYOD/school provided device is brought to school each day unless otherwise informed.
- Ensure their BYOD/school provided device has the Apps/software installed as requested by the school and maintain software upgrades.
- Abide by the policy and to report any concerns regarding breaches of the policy to a member of staff

Parents:

It is vital that parents and the school work together to ensure that all students are safe online and to make students aware of the serious consequences of failing to follow the policy.

Parents have a responsibility to talk to their children about values and the standards that their children should follow regarding the use of the Internet as they would in relation to the use of all media information sources such as television, telephones, movies, radio and social media.

Parents can help by making sure their child understands the school's policy and, above all, how seriously the

school takes incidents of misuse of technology and cyberbullying.

If parents believe their child is the victim of cyberbullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.

Parents should contact the school as soon as possible if they have any concerns regarding the use of technology in school. A meeting can then be arranged with a member of the Senior Leadership Team.

6 **Applicable to:**

Whole school community

7 **Related Documents**

Safeguarding and Child Protection Policy

Acceptable Use of Technology Agreement

8 **Implementation Date:** August 2021

Review Date: As required

Appendix 1

Risks to students while engaged in E-Learning

The potential harm or risk	Mitigation
Impact on quality of life, physical and mental health and relationships.	Teachers need to identify when online behaviors stop being fun and begin to create anxiety, including that there needs to be a balance between time spent on and offline. Teachers should: • Plan for a lower volume of work from students or allow for extended timescales • Provide for reasonable deadlines • Plan screen-based and non-screen-based activities to achieve a healthy screen-time balance • Set marking expectations and standards, which may be different from normal Teaching could include: • helping students to evaluate critically what they are doing online, why they are doing it, and for how long (screen time). This could include reference to technologies that help them to manage their time online, monitoring usage of different apps etc, • helping students to consider quality vs quantity of online activity, • explaining that students need to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or the fear of missing out, • helping students to understand that time spent online gives users less time to do other activities. This can lead to some users becoming physically inactive, • explaining that isolation and loneliness can affect students and that it is very important for students to discuss their feeling with an adult and seek support. • Providing information of where to get help

Safeguarding during online learning	Teachers should: • refer to the update Safeguarding policy • be vigilant and consider safeguarding obligations. Report any safeguarding incidents or potential concerns according to the safeguarding policy • Ensure online tuition follows best practice whenever possible e.g. 2 members of staff involved or a parent/carer present during the session • Remind students of who they can contact within the school for help or support.

Teachers inadvertently sharing personal information due to what can be seen	Teachers should: • blur the background or use background screen controls to share a suitable background image • set up their workspace in a suitable location where they can engage in teaching without distractions • mute their microphone as necessary
Students inadvertently sharing personal information due to what can be seen or heard on the	Teaching could include: • provide advice to families regarding setting up a suitable workspace. A child's bedroom is not a suitable location • encouraging students to mute their microphone when not speaking. (the teacher should be familiar with how to control/disable the microphone or video/camera of users
During lessons students use the chat facility	Teaching could include: • setting clear rules and boundaries for using chat • turn off this option when not required for the lesson
Live streaming of lessons	Teachers should: • Only use school-registered accounts, never personal ones • Don't use a system that your SLT has not approved • Ensure you edit the settings first (who can chat? who can start a stream? who can join?) • Keep to your scheduled start time, never start without other colleagues being aware • Keep a log of everything - what, when, with whom and anything that went wrong • Avoid one-to-ones unless pre-approved by SLT • If you don't understand the system, if it won't be safe or reliable, if teaching won't be enhanced, DON'T DO IT.
During lessons, students accessing content outside of the recommended Age restrictions.	Teaching could include: • that age verification exists and why some sites require a user to verify their age. For example, online purchasing of certain age restricted materials. • why age restrictions exist - for example, they provide a warning that the site may contain disturbing material that is unsuitable for younger viewers, • helping students understand how this content can be damaging to under-age consumers, • the age of digital consent- the minimum age (13) at which young people can agree to share information and sign up to social media without parental consent.

Students may develop inappropriate online behavior	Teaching could include: • helping students to understand what acceptable and unacceptable online behavior looks like. Set ground rules. Explain that the same standard of behavior and honesty applies on and offline, including the importance of respect for others. • Create a safe space by reminding students about the ground rules in the introduction to each session, for example who can speak and when. Create a safe space by reminding students about the ground rules in the introduction to each session, for example who can speak and when. • Students should be taught how to recognize unacceptable behavior in others.
Recording of live online sessions	Due to cultural sensitivities great care should be taken when recording sessions. Teachers should: • make an announcement at the beginning of the session to state that the session will be recorded and seek everyone's permission. Parents who do not give permission should disable their video/camera • make a note of the conference timing and who participated, including those that arrived/departed early or late • set clear expectations/restrictions about onward sharing
Student's content being used, stored and potentially used against them in the future.	Students need to be made aware of what happens to information, comments or images that are put online. Teaching could include: • what a digital footprint is, how it develops and how it can affect future prospects such as university and job applications, • how cookies work, how content can be shared, tagged and traced, • how difficult it is to remove something a user wishes they had not shared, • ensuring students understand what is illegal online, especially what may in some cases be seen as "normal" behaviors. This could include copyright, sharing illegal content such sharing any explicit images of a child even if created by a child.

Students believing disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading, or exaggerated. Teaching could include explaining: • disinformation and why individuals or groups choose to share false information in order to deliberately deceive, • misinformation and being aware that false and misleading information can be shared inadvertently, • online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons

	• that the viral nature of this sort of content can often appear to be a stamp of authenticity and therefore why it is important to evaluate what is seen online, • how to measure and check authenticity online, • the potential consequences of sharing information that may not be true.
Students being exposed to fake websites and scam emails/messages	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other gain. Teaching could include: • how to look out for fake URLs and websites, • ensuring students understand what secure markings on websites are and how to assess the sources of emails, • explaining the risks of entering information to a website which is not secure, • what to do if harmed/targeted/groomed as a result of interacting with a fake website or scam email. Who to go to and the range of support that is available.
Students being the targets of fraud	Fraud can take place online and can have serious consequences for individuals and organizations. Teaching could include: • what identity fraud, scams and phishing are, • that children are sometimes targeted to access adults data, for example, passing on their parents or carers details (bank details, date of birth, etc). Therefore, there is a need to keep everyone's information secure not just their own,

Students being the targets of Password phishing	Password phishing is the process by which people try to find out your passwords so they can access protected content. Teaching could include: • why passwords are important, how to keep them safe and that others may try to trick you to reveal them, • what to do when a password is compromised or thought to be compromised. • explaining how to recognize phishing scams, for example those that seek to gather login in credentials and passwords,
Students revealing personal data	Online platforms and search engines gather personal data. This is often referred to as 'harvesting' or 'farming'. Teaching could include: • how cookies work,

	• how data is farmed from sources which look neutral, for example websites that look like games or surveys that can gather lots of data about individuals, • how, and why, personal data is shared by online companies. For example data being resold for targeted marketing by email/text (spam), • how students can protect themselves, including what to do if something goes wrong (for example data being hacked) and that acting quickly is essential,
Students being persuaded to extend their screen time due to persuasive design	Many devices/apps/games are designed to keep users online for longer than they might have planned or desired. Teaching could include: • explaining the dangers of too much screen time and providing recommended guidance • explaining that the majority of games and platforms are businesses designed to make money. Their primary driver is to encourage users to be online for as long as possible to encourage them to spend money (sometimes by offering incentives and offers). • how designers use notification to pull users back online.
Students changing privacy settings	Almost all devices, websites, apps and other online services come with privacy setting that can be used to control what is shared. Teaching could include: • explaining the importance of privacy setting and setting clear rules and consequences • explaining that privacy settings have limitations, for example they will not prevent someone posting something inappropriate
Students being exposed to targeted adverts and content	Teachers should avoid using open sources which display adverts. Teaching could include: • how adverts seen at the top of online searches and social media feeds have often come from companies paying to be on there and different people will see different adverts, • how the targeting is done, for example software which monitors online behavior (sites they have visited in the past, people who they are friends with etc) to target adverts thought to be relevant to the individual user.

Students suffering abuse (online)	Teaching could include: • explaining about the types of online abuse including harassment, bullying, sexual, trolling and intimidation,

	• how to respond to online abuse including how to access help and support • how to respond when the abuse is anonymous, • discussing the potential implications of online abuse, including implications for victims, • being clear what good online behaviors do and don't look like. • explanation of when online abuse can cross a line and become illegal, such as forms of hate crime and blackmail.
Students taking part in unauthorized 'challenges' and dares	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching could include: • explaining what an online challenge is and that while some will be fun and harmless, others may be dangerous and or even illegal, • how to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why, • explaining to students that it is ok to say no and not take part, • how and where to go for help if worried about a challenge, • understanding the importance of telling an adult about challenges which include threat or secrecy ('chain letter' style challenges).
Students being exposed to content which incites	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching could include: • ensuring students know that online content (sometimes gang related) can glamorize the possession of weapons and drugs, • explaining that to intentionally encourage or assist an offence is also a criminal offence, • ensuring students know how and where to get help if worried about involvement in violence.
Students accessing sites that expose them to fake profiles or grooming	Teaching could include: • emphasizing the importance of only accessing approved Apps and site • explaining that in some cases profiles may be people posing as someone they aren't (i.e. an adult posing as a child) or may be "bots" (which are automated software programs designed to create

	• explaining the importance of maintaining boundaries in friendships with peers and also in families and with others • how and where to report if contacted by an unknown adult/child
Students deliberately or inadvertently live streaming themselves	Live streaming (showing a video of yourself in real-time online either privately or to a public audience) can be popular with children but it carries risk when carrying it out and watching it. Teaching could include: • explaining the risks of carrying out live streaming. These include the potential for people to record live streams without the user knowing and content being shared without the user's knowledge or consent. As such students should think carefully about who the audience might be and if they would be comfortable with whatever they are streaming being shared widely, • online behaviors should mirror offline behaviors and considering any live stream in that context. • Students should not feel pressured to do something online that they wouldn't do offline. Consider why in some cases people will do and say things online that they would never consider appropriate offline, • explaining the risk of watching videos that are being live streamed, for example there is no way of knowing what will come next and so this poses a risk that a user could see something that has not been deemed age appropriate in advance.
Students being exposed to 'perfect images' and the impact on confidence (including body confidence)	Teachers need to be aware of the impact of comparisons to 'unrealistic' online images. Teaching could include: • explaining and exploring the use of image filters and digital enhancement, • exploring the role of social media influencers, including that they are paid to influence the behavior (particularly shopping habits) of their followers • discussing photo manipulation including discussions

Keeping up to date with latest risks and threats.	The online world develops and changes at great speed. New risks, opportunities, challenges are appearing all the time. Difficult for schools to stay up to date with the trends and related threats. Teachers should focus on the underpinning knowledge and behaviors that can help students to navigate the online world safely and confidently regardless of the device, platform or app.