CONTENT AND SECURITY AWARENESS - 2026

At Substance Global, we understand both the privilege we have and the responsibility we bear in working on / with the highest of value and sensitive client IP and content - of all kinds, but especially on/with pre-release content (i.e. that which is not yet in the public domain).

In addition to the principles previously agreed to (in contracts of employment and our employee handbook), this document contains further guidelines to be shared with new starters at Substance and to be revisited on a not less than annual basis, in order to refresh our understanding of how to conduct ourselves and to raise awareness of best practices in protecting the IP we may encounter..

In short - this document seeks to succinctly remind all staff who handle and interact with content of the simple but important steps we must follow to best ensure its safeguarding, and to record our acknowledgement of such.

CONTENTS:

1) CONTENT AND IT SECURITY 101

What do we mean by 'content'?
Though we may usually mean audio / video when discussing content, images, artwork, scripts and media plans are all also considered content and are to be protected under this policy. 'Sensitive content' is anything that is not in the public domain and therefore is to be handled and treated with additional caution and care.

Simple rules to always follow

- **Local storage** - you should never store content of any kind locally on your computer - that is what Box and our google drive are there for.
- **Passwords** - Complex and unique passwords must be used (this is mandated by IT policy) and never shared. Passwords can only be changed once per day, by policy.
- **Email usage -** Never email content directly - instead please use applications for transfer (Box / drive) - and make sure the intended recipient is correct
- **If ever you're not sure about something -** always check with the security team at security@substanceglobal.com

2) PHYSICAL SECURITY

Simple rules to always follow
In the office

- Your keycard is yours alone and not to be shared with colleagues.
- Permission to bring guests to the office must be sought in advance. When in the office, guests are to be signed in with our log book and should complete an NDA. Guests are to be accompanied at all times while on the premises.

- When working in the office and if accessing/working on sensitive content, then you are not to use your mobile device.
- Watching / accessing sensitive content in the office is restricted to those who need to view/access as a business requirement.

At home

- If working from home, we must do so in a safe and secure environment, making sure that what we are working on is never overlooked by friends or family.
- If you have remote access to pre-release content of any kind while working from home, this is not to be viewed by / discussed with anyone in your household.
- Taking sensitive and pre-release content (including on encrypted drives) from the office is expressly forbidden, with the exception of when we are returning such to clients via courier.

Working elsewhere (public areas / while in transit)

- With no exceptions, sensitive and pre-release content can never be accessed when in public places, while connected on public wifi networks, or while in transit.
- Additional care should also be taken to avoid your work and emails being overlooked.

3) USE OF SOCIAL MEDIA / TALKING ABOUT WHAT YOU DO AT SUBSTANCE

You must never post about, or make reference on Social Media to, nor in conversation with friends/family, any pre-release content on which you may be working. This extends to both tiles and clients alike, and includes expressing opinions on the relative merits of anything that is not yet in the public domain but, in that instance, it is still best to apply **the Thumper Rule** - 'if you can't say something nice, don't say nothing at all'.

4) USE OF PERSONAL EQUIPMENT, INCLUDING MOBILE PHONES

Personal computer equipment - Use of personal computer equipment, including to access emails and shared/cloud drive content, is prohibited as standard, except under exceptional and limited circumstances, when express permission must be sought and granted in advance.

NOTE - Access to client content on personal computer equipment is prohibited under any circumstance.

Mobile phones

Use of mobile devices at/for work purposes may be necessary, on an occasional basis, but the recording of (including images / screenshots / videoing) any content you may have access to is expressly prohibited, as is use of mobile phones while working in the studio / content production area.

5) WHISTLEBLOWING / REPORTING

Just as we must all take our responsibilities for secure handling of content seriously at all times, it is also each of our responsibilities to report any suspected breaches of these guidelines, accidental or otherwise, by yourself or by colleagues. Such should please be reported to the Security Management Team (security@substanceglobal.com) immediately, via this link: https://substanceglobal.com/grievance-whistleblower-policy so that we can react quickly and appropriately.

6) ACKNOWLEDGEMENT

"I acknowledge that I have read, understood and will adhere to the above guideline at all times."

NAME **SIGNED**