Sky and Sky Studios Commissioned Productions

Pre-release Content Security Guidelines

This document outlines pre-release content security requirements that need to be followed across all our productions to keep our content and assets safe. It is intended to be a used across all productions phases and it aims to address security controls and expectations when handling (i.e., creating, receiving, viewing, storing, sending, and/or sharing) pre-release/pre-TX content.

This guidance document is to be shared with all cast and crew, suppliers and companies engaged on the production at the earliest opportunity. Recipients should read and understand what is relevant to them before starting their work and liaise with their production company contact for any guidance and clarification.

Every individual and company engaged in the production is responsible for adhering to this guidance at a minimum.

Pre-release content is defined as all materials and assets related to the film or television making process prior to their intended release, including, but not limited to: scripts, sides, breakdowns, dailies, rough cuts, final cuts, trailers, promos, behind the scenes footage, audio elements, key art, still images, posters, auditions, plot points, spoilers, legal, finance, production document deliverables and other personal or confidential information. Note that pre-release content includes personal information and other information that must be kept confidential and secure even after release.

Our objective is to empower everyone to securely handle all pre-release Sky and Sky Studios content.

Standard Security Requirements

your laptop, phone and other devices used whilst working on the production	• Must be password protected/require authentication to unlock. A 12 character password is recommended • Must be kept in a secure location at all times • Must not be left unlocked and unattended • Must be used by you exclusively, and not shared with other team members, family or friends
everyday security	• Keep things confidential – including from family and friends • If you can work in a room where you can close the door, do so • Where you have been asked to use a specific piece of software, manage documents or information in a specific way for this production please do so; do not save documents to your desktop/personal storage • Where provided, use a company email address at all times, do not use your personal account. • Follow policies provided to you, including the acceptable use policy
Working in public locations / travelling	• Do not watch contentious, sensitive, or highly confidential dailies, assemblies, cuts or screeners in a place where your screen can be seen • If you must watch pre-release content in a public place, always use headphones and if you have a screen protector, please use it • Public or open Wi-Fi networks should not be used. If you must use the Wi-Fi, use the private (password protected) network and VPN; or wait until a location you know has a secure connection • When travelling always keep your laptop and devices on your person. Do not leave them unattended
Working in High-Risk environments or Overseas	• Specific guidance will be provided to you by your production team which will be discussed and approved by Sky. This will list any specific additional steps you need to follow to stay safe and secure.
Insurance	• The production must have Cyber Security Insurance cover in place

Pre-production and Production Management	• Project names are to be used in lieu of titles for productions where appropriate • Physical security must be considered for all aspects of production with access to offices, filming spaces, edits and storage (fixed or mobile) restricted to an individual basis e.g. electronic security access control • Call-sheets and any documents with secure information that needs to be shared across production, should be watermarked and password protected • Distribution lists for scripts/sides, schedules and movement orders are to be regularly updated ensuring information is not shared in error • On set/office Wi-Fi/4G/5G networks should be set up and managed by reputable contractors, encrypted, and password protected. • Couriers and bookings should be timely to ensure rushes are not sat waiting in goods-in or front desks. Reputable couriers must be used.
Media Asset Management	• Media management workflows are to be documented before production commences, and are to ensure device security, physical and cloud security are considered throughout • Drive logs should be password protected and only distributed on a need to know basis. • File and folder naming conventions should be applied consistently throughout to reduce risk of duplication or loss • All drives and any media used to capture, transfer or store content must be encrypted, with passwords shared securely only with those required to directly access the contents
Post-production and delivery	• • Consideration should be given to management of files and storage for sensitive or contentious content, or highly confidential shows. Shared storage is not permitted, designated (partitioned) storage is mandatory. • Any post production work undertaken "remotely" or "from home" must be in a fixed location that is physically secure. E.g. in a home studio not from a coffee shop • Any post production work undertaken "remotely" or "from home" must employ secure remote editing capabilities such as remove desktop or virtual desktop wherever possible, personal drives and storage must not be used • Couriers and bookings should be timely to ensure rushes are not sat waiting in goods-in or front desks. Reputable couriers must be used • Completed assets should be shared with Sky and partners only via the approved file transfer routes
Suppliers and vendors	• Sky preferred suppliers must be used in the first instance, including for any post-production, PR, marketing or other work that involves handling of audio/video assets • Work must not be sub-contracted by your chosen supplier without consultation and approval. • Where a post-production, VFX or localisation supplier is not listed on Sky's preferred list, it must be checked for TPN accreditation or DPP standard adherence and approved by Sky in writing before contracting • All suppliers must warrant that they can meet these Content Security Guidelines as a minimum standard whilst engaged on the production
Tools and software applications	• Applications used must be approved by the production company in line with their software policy.

	• Individual’s access to all provided software or shared document storage must be routinely checked with leavers access revoked on the day they finish on production
Sharing cuts and viewing copies	• Only use your production’s approved viewing platform to upload and share viewing copies or screeners. • Share with named individuals only and never forward on links. Wherever possible, establish an approved distribution list. • If sharing with a company, ensure you share to their company email address – links should not go to personal emails. • Password protection, watermarking and link time-out must be in place as standard. • If you are unsure as to whether someone should receive viewing copies, don’t hesitate to check with a supervisor or manager.
Delivery	• For final delivery, follow the guidance as provided by Sky or your distributor. This will reduce the risk of issue or file corruption and/or interception.
Archiving	• Full back ups of all assets are to be kept securely for the duration of the contractual licence period.
Loss or Theft	• Report any suspected loss or theft of assets or information as quickly as possible to the Head of Production or your Production Executive at Sky
Generative AI	• Use of Generative AI tooling or software on any aspect of production or production workflows must be discussed and cleared in advance in writing with Sky.

Enhanced Content Security Measures

Each production will go through a content security review in line with Editorial Specification (EdSpec) approval. Any enhanced safety requirements will be addressed on a case-by-case basis, and specific risks addressed with the enhanced measures across any of the categories listed above.