



Digital Asset Management Policy

Part of the policy Framework

Our Mission

To promote high standards of Western Equitation
and stimulate the growth of these riding disciplines



Document Metadata

Policy Title	Digital Asset Management Policy
Document Ref.	WES-POL-0018
Version	1.0
Date Published	04/11/2025
Review Date	04/11/2027
Owner (Role)	Secretary
Author	Dan Gwalter
Approved By	Secretary
Confidentiality	Public
Status	Published

Contents

Document Metadata	1
1. Purpose	3
2. Scope	3
3. Definitions	3
4. Policy Statement	4
5. Roles and Responsibilities	4
6. Policy Detail / Procedures	4
7. Related Policies and References	6
8. Compliance and Breach Handling	6
9. Review and Version Control	6
10. Approval Record	6

1. Purpose

This policy sets out how the Western Equestrian Society (WES) manages its digital assets — including logos, templates, images, video, and branded materials — to ensure consistency, legal protection, and ease of access for those who need them.

It also covers file naming, version control, and responsible use of shared content across the Society.

2. Scope

This policy applies to:

- All digital files used to represent or deliver the work of WES
- Content held in shared drives, web platforms, and cloud-based systems
- Council members, Officers, volunteers, event leads, and contractors who use or manage digital assets

It covers:

- File types and categories
- Branding assets (e.g. logos, templates)
- Photos and videos
- Version control and naming conventions
- Access, storage, and platform usage

Commented [1]: @dan@wes-uk.com Suggest you say emails are excluded and refer to the Data retention policy
Assigned to dan@wes-uk.com

3. Definitions

- **Digital Asset:** Any file used in the digital delivery of WES communications, events, governance, or branding
- **Authorised User:** Anyone granted access to official WES files for a defined role or function
- **Asset Register:** A central record of core WES digital assets (templates, logos, forms, brand files)
- **Shared Drive:** The central Google Workspace drive used to store and distribute WES digital assets

4. Policy Statement

WES recognises digital content as a key Society resource and branding tool. Files must be stored centrally, named consistently, and made available to the right people — not copied and lost across personal drives.

Digital assets will be created, stored, and retired in a structured way, with role-appropriate access and clear version control.

5. Roles and Responsibilities

Role	Responsibility
Secretary	Maintains the Asset Register and Data Room structure; oversees access control and versioning
PR / Comms Lead	Manages official branding assets, imagery, and promotional templates
Treasurer	Manages financial templates and standard forms
Event Leads	Use only approved assets when publishing event materials or results
All Users	Avoid duplication, uncontrolled file storage, or editing master templates

6. Policy Detail / Procedures

6.1 Types of Digital Asset Covered

- Logos and branding kits (incl. colour values, fonts)
- Templates for board packs, proposals, meeting minutes, judging sheets
- Social media graphics and event banners
- Photography and video files
- Membership forms and PDFs
- Web-ready content (text, banners, policies)

6.2 Access and Storage

- All official assets will be stored in the WES Shared Drive under the **Digital Assets** directory
- Users requiring access must request it from the Secretary or designated folder owner
- Files must not be downloaded and edited offline unless necessary — use “Make a copy” in Drive
- Outdated versions must be deleted or moved to the **Archive** subfolder

6.3 File Naming and Version Control

- Standard naming format:
YYYYMMDD-Asset-Type-Title-vX.X
Example: 20250710-Template-BoardPack-v1.2
- Major changes = increment first digit (v2.0), minor edits = second digit (v1.1 → v1.2)
- Master files must carry “_MASTER” in the title
- Avoid using personal initials, vague file names, or duplicates

6.4 Photography and Video

- Images used in promotional materials must be appropriately credited and rights-cleared
- Consent must be in place for recognisable individuals (especially youth or vulnerable adults)
- Event photos stored centrally should be tagged with event name and date in folder title
- Video content should be held in YouTube, Google Drive, or another approved platform with shared access

6.5 Use of External Tools and Links

- Canva and SurveyMonkey accounts used for WES purposes must be linked to the WES email identity
- External links to assets must not be made public unless authorised by the Secretary or PR Lead
- Expired or broken links must be reported and removed from circulation

6.6 Asset Register

- A rolling register of core WES digital assets will be maintained and stored in the Templates and Tools folder
- It will list:
 - File title and version
 - Owner
 - Last updated date
 - Purpose and approved use

6.7 Departing Officers and Volunteers

- All digital content must be returned or moved to the Shared Drive
- No WES content should remain on personal devices after a role ends
- Shared access permissions will be reviewed quarterly and revoked when roles change

7. Related Policies and References

- Policy Review and Maintenance Policy

- Data Protection (GDPR) Policy
- Confidential Records Protocol
- Templates and Tools Index
- WES Asset Register (Templates folder)
- Data Retention policy

8. Compliance and Breach Handling

Use of incorrect or outdated branding, duplicate versions of templates, or failure to store records centrally may result in process duplication or reputational risk.

Persistent non-compliance may result in access being restricted or referred for governance review.

9. Review and Version Control

Version	Date	Author	Changes Made
0.1	18/07/2025	DG	Initial policy draft
0.5	08/10/2025	DG	Changes following chairmans review
1.0	04/11/2025	DG	Published

10. Approval Record

Approved By	Date	Notes
Full Council	04/11/2025	Approved for immediate use