IT and Email Access 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	**IT and Email Access Policy**
Document Ref.	WES-POL-0019
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

1. Purpose

This policy sets out how WES manages access to its digital systems, email communication channels, and file-sharing infrastructure. It ensures that Society data is accessible to the right people, protected against misuse, and handled consistently — even in a non-centralised environment.

Given that WES operates primarily through a shared Google Workspace, this policy clarifies expectations for data handling, access rights, and responsible use of personal email when acting in an official capacity.

2. Scope

This policy applies to:

- All Council members, Officers, and volunteers with access to WES digital systems
- Anyone acting in an official capacity for the Society who sends or receives information relevant to WES operations
- All shared files, folders, forms, and tools used within the WES Google Workspace

It includes:

- Use of personal email accounts
- Access to the WES Shared Drive (Data Room)
- Permissions for templates, documents, and folders
- File naming and ownership expectations
- Role transitions and access withdrawal

3. Definitions

- **WES Shared Drive**: The Google Workspace drive that houses governance, event, and operational records
- **Authorised User**: A person who has been granted edit or view access to shared materials in the course of their WES role
- **Personal Email**: Any email address not issued or managed centrally by WES (e.g. Gmail, Outlook, Yahoo)
- **Sensitive Data**: Any personal, disciplinary, safeguarding, or confidential Council material

4. Policy Statement

WES does not issue official email addresses. Council and volunteers use their personal email accounts to carry out Society work. This is acceptable but comes with specific responsibilities around data control, storage, and tone.

All WES records must be stored centrally in the WES Shared Drive, not within personal email folders or devices. When acting in an official capacity, Officers must avoid email content that would be problematic if disclosed under GDPR or a future Subject Access Request.

5. Roles and Responsibilities

Role	Responsibility
Secretary	Manages the Shared Drive structure; grants and removes access as needed
All Officers	Use personal emails responsibly; store all records in the Data Room
Chairperson	Oversees communication tone and conflict management where required
Departing Officers	Ensure timely handover and revocation of permissions

6. Policy Detail / Procedures

6.1 Email Use in Official Capacity

- All formal communications (e.g. meeting invites, decisions, policies, complaints, finance) must be copied or saved to the appropriate Shared Drive folder
- Emails should be written with the awareness that they may be disclosed under GDPR
- Personal commentary, speculative discussion, or informal opinions should be avoided in long-running threads
- Where possible, decisions should be captured via agreed meeting minutes or Google Docs rather than left in email trails

6.2 Access to the WES Shared Drive

- Role-holders may be granted ‘Viewer’ or ‘Editor’ access to specific folders
- Full access to the drive is restricted to the Secretary and a small number of core Officers
- Permissions are issued based on role, not personal preference
- Access will be reviewed quarterly and revoked when roles end

6.3 Folder Ownership and File Management

- All key documents must be created within or moved to the relevant Shared Drive folder

- Do not store WES materials in personal drives or desktop folders
- Templates should be duplicated using “Make a copy” — not overwritten
- Master copies should carry the _MASTER tag and versioning info in the filename

6.4 Transitions and Offboarding

- When a role-holder steps down, their access will be removed by the Secretary within 7 days
- Any files stored in personal locations must be returned to the Shared Drive or deleted
- Shared folder permissions will not be transferred between individuals without Secretary approval

6.5 Google Workspace Standards

- Only Google Workspace-compatible formats should be used when creating templates (Docs, Sheets, Forms)
- External tools (e.g. Canva, SurveyMonkey) must be linked to the WES workspace or controlled by the Secretary
- Shared links should always default to “Restricted” access unless explicitly authorised

6.6 Shared Link Risks

- Council members must avoid sharing open access links via social media or email lists
- Any shared link used to communicate with external parties must be time-limited or access-controlled
- Misuse or accidental sharing of a confidential file must be reported immediately to the Secretary

7. Related Policies and References

- Digital Asset Management Policy
- Data Protection (GDPR) Policy
- Confidential Records Protocol
- Data Breach Reporting Procedure
- Policy Review and Maintenance Policy

8. Compliance and Breach Handling

Failure to store records centrally, protect sensitive data, or manage email content appropriately may result in:

- Data loss or inaccessibility
- Reputational or legal risk
- Disciplinary action in line with the WES Council Code of Conduct

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