Data Breach Reporting Procedure

v1.0 | Published

Western Equestrian Society | wes-uk.com

Contents

Data Breach Reporting Procedure

Document Metadata

Policy Title	Data Breach Reporting Procedure
Document Ref.	WES-POL-0016
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

1. Purpose

This policy defines how the Western Equestrian Society (WES) will respond to a **personal data breach**. It ensures that incidents are:

- Recognised quickly
- Handled consistently
- Logged appropriately
- Mitigated effectively
- Reported to relevant parties if required

It protects the rights of individuals whose data may be affected, while limiting legal and reputational risk to the Society.

2. Scope

This procedure applies to:

- All personal data held by WES (electronic or physical)
- Council members, Officers, or volunteers with access to personal data
- All data processing platforms used by WES (e.g. Member Mojo, SurveyMonkey, Google Workspace)

It covers incidents involving:

- Loss or theft of data
- Unauthorised disclosure or access
- Accidental or unlawful destruction
- Sending data to the wrong person
- Compromised user accounts or systems

3. Definitions

- **Personal Data Breach**: A security incident that results in accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data
- **Data Subject**: The individual whose personal data is involved
- **ICO**: The Information Commissioner's Office, the UK regulator for data protection
- **Data Controller**: The organisation responsible for determining how and why data is used (WES)

4. Policy Statement

WES takes all data breaches seriously. Every breach must be reported immediately, logged by the Secretary, and assessed to determine whether:

- The breach must be reported to the ICO
- Affected individuals need to be notified
- Internal remedial or disciplinary action is required

No individual should attempt to manage a breach in isolation or delete evidence.

5. Roles and Responsibilities

Role	Responsibility
Secretary	Acts as Data Lead; maintains breach log; coordinates response and reporting

Chairperson	Supports communications, escalation, and oversight of serious breaches
Data Holder	Any Officer, volunteer, or Council member with access to personal data
Treasurer	Ensures breaches affecting financial data are reported and mitigated

6. Policy Detail / Procedures

6.1 Identifying a Breach

Common examples include:

- Sending an email or document containing personal data to the wrong person
- Accidental inclusion of sensitive information in a newsletter or bulk email
- Loss or theft of a device containing WES records
- Disclosure of member or disciplinary details without lawful basis

6.2 Immediate Action

Any individual who becomes aware of a potential breach must:

- Report it to the Secretary **immediately** (email, phone, or in person)
- Avoid deleting or modifying evidence (e.g. email threads)
- Provide basic details: what happened, when, what data was involved, and who was affected

6.3 Assessment

The Secretary will:

- Log the incident in the **Data Breach Register**
- Confirm whether personal data was involved
- Assess likely impact and whether individuals can be identified
- Classify the breach using the WES Risk Matrix (Low / Moderate / High)

6.4 Internal Mitigation

WES will take appropriate steps to:

- Limit further disclosure (e.g. recalling an email, correcting access rights)
- Secure affected systems or files
- Engage with those affected to provide reassurance or information
- Assess whether additional training or process change is needed

6.5 Notification Requirements

A breach must be reported to the ICO **within 72 hours** *if* there is a risk to individuals' rights or freedoms (e.g. reputational harm, identity theft risk).

The Secretary, in consultation with the Chair, will decide if notification is required. If in doubt, a conservative approach will be taken.

Affected individuals may also be notified if:

- There is a high risk to their rights
- The data involved is sensitive (e.g. disciplinary, financial, medical)
- WES wishes to demonstrate transparency and accountability

6.6 Documentation

Each breach log entry will include:

- Description of the incident
- Dates of discovery and reporting
- Scope and nature of data affected
- Actions taken
- Whether the ICO or individuals were notified
- Lessons learned or policy impact

7. Related Policies and References

- Data Protection (GDPR) Policy
- Subject Access Request Procedure
- Risk Management Policy
- Confidential Records Protocol
- ICO Breach Notification Guidelines
- WES Data Breach Register (Templates and Tools folder)

8. Compliance and Breach Handling

Failure to report a data breach may itself be treated as misconduct or a governance breach. All Officers and volunteers must act swiftly and openly if they suspect a breach has occurred. Attempting to conceal a breach may result in disciplinary action.

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