Esports Wales

Cyber Security Policy

Status: Board-approved policy
Applies to: Directors, Staff, Volunteers, Coaches, Officials, Members, Partners
Owner: Board of Directors
Cyber Security Lead: Board-appointed Director / Senior Officer
Data Protection Lead: Board-appointed Director / Senior Officer
Safeguarding Lead: Designated Safeguarding Lead (DSL)
Review cycle: Annual
Next review due: 12 months from adoption

---

1. Purpose

This policy sets out how **Esports Wales CIC** ("the Company") protects its **digital systems, data, and online platforms** from cyber security threats.

It exists to:

- protect personal and sensitive data
- reduce the risk of unauthorised access, loss, or disruption
- support safe online participation in esports
- meet legal, safeguarding, and governance obligations
- promote responsible and secure digital behaviour

---

2. Scope

This policy applies to:

- all digital systems, devices, and platforms used by Esports Wales
- online services, communication tools, and cloud systems

- personal devices used to access Esports Wales systems (where permitted)

It applies to all individuals with access to Esports Wales systems.

---

3. Cyber Security Principles

Esports Wales is guided by the following principles:

- **Confidentiality** – data is accessed only by authorised users
- **Integrity** – data is accurate and protected from unauthorised change
- **Availability** – systems are reliable and resilient
- **Proportionality** – controls reflect risk and organisational size
- **Shared Responsibility** – cyber security is everyone's responsibility

---

4. Key Cyber Security Risks

Esports Wales recognises risks including:

- unauthorised access or hacking
- phishing or social engineering attacks
- malware, ransomware, or viruses
- loss or theft of devices
- misuse of accounts or credentials
- online harassment or platform abuse

---

5. Access Control & Authentication

5.1 Access to systems will be:

- limited to authorised individuals
- role-based where possible

5.2 Individuals must:

- use strong, unique passwords
- not share login credentials
- log out of shared or public devices

Multi-factor authentication should be used where available.

---

6. Devices & Systems

6.1 Esports Wales devices must:

- use up-to-date software and security patches
- have appropriate antivirus or endpoint protection

6.2 Personal devices:

- must meet minimum security standards
- must not store sensitive data unless authorised

---

7. Online Platforms & Esports Systems

7.1 Platforms used for competition, communication, or streaming must:

- be approved where appropriate
- comply with Esports Wales safeguarding and data protection policies

7.2 Platform access must be:

- restricted to appropriate roles

- reviewed periodically

---

8. Data Security & Encryption

8.1 Personal and sensitive data must be:

- stored securely
- transmitted using secure methods

8.2 Sensitive data must not be:

- shared via unsecured email or messaging apps
- stored on personal cloud accounts

---

9. Cyber Incidents & Breaches

9.1 A cyber security incident includes:

- data breaches
- system compromise
- suspected unauthorised access

9.2 All incidents must be:

- reported immediately to the Cyber Security or Data Protection Lead
- recorded and assessed
- escalated where required

(See **0801 Data Protection (UK GDPR) Policy**)

---

10. Safeguarding & Cyber Security

10.1 Cyber security is critical to safeguarding, particularly where:

- children and young people are involved
- online communication or streaming is used

10.2 Cyber incidents that present safeguarding risk must be:

- escalated immediately
- managed under safeguarding procedures

(See **0213 Online Safety & Digital Safeguarding Policy**)

---

11. Training & Awareness

Esports Wales will:

- promote cyber security awareness
- provide guidance on recognising threats
- ensure key roles understand cyber risks

---

12. Roles & Responsibilities

12.1 Board of Directors

- holds ultimate accountability for cyber security governance

12.2 Cyber Security Lead

- oversees implementation of this policy
- responds to cyber incidents
- reports significant risks to the Board

12.3 All Users

- must comply with this policy
- must report suspected cyber threats or incidents

---

13. Compliance & Enforcement

Failure to comply with this policy may result in:

- restriction or removal of system access
- disciplinary or governance action
- referral to external authorities where appropriate

---

14. Linked Policies & Procedures

This policy must be read alongside:

- **0801 Data Protection (UK GDPR) Policy**
- **0802 Privacy Policy**
- **0803 Data Retention & Disposal Policy**
- **0213 Online Safety & Digital Safeguarding Policy**
- **0701 Disciplinary Policy & Procedure**

---

15. Review

This policy shall be reviewed:

- annually
- following cyber security incidents
- following changes in technology or guidance

16. Adoption

This Cyber Security Policy was approved by the Board of Directors of **Esports Wales CIC**.

Date approved: ___02/03/2026_____

Signed (Chair):___  ____