CIMSPA®

Data governance framework

Contents

PUBLISHED BY:
The Chartered Institute for the Management of Sport and Physical Activity
Incorporated by Royal Charter
Charity Registration No. 1144545
www.cimspa.co.uk

V1: March 2026

1. Purpose

The CIMSPA Data Governance Framework for the Sport and Physical Activity Workforce Observatory establishes clear principles and guidelines for managing workforce data within CIMSPA.

This framework ensures data quality, security, accessibility, and compliance with legal and regulatory standards, supporting strategic decision-making and promoting data-driven workforce development.

By adopting this Data Governance Framework, CIMSPA aims to foster a culture of responsible data management, ensuring that workforce data is handled in a manner that supports organisational goals while complying with relevant legal and regulatory requirements. This framework will enhance the quality, security, and usability of workforce data, enabling CIMSPA to make data-driven decisions that optimise workforce development and contribute to broader industry best practices.

The framework will:

- ensure data quality, security and accessibility to support workforce development and strategic initiatives
- maintain compliance with UK laws and international regulations, including GDPR, the Data Protection Act 2018, and National Data Strategy Guidelines
- foster a culture of transparency and accountability, ensuring data use aligns with CIMSPA's mission and ethical standards
- mitigate risks associated with data management, including breaches, unauthorised access, and data inaccuracies
- enhance workforce insights by ensuring secure, reliable, and well-structured data for research, policymaking, and workforce planning.

This framework applies enterprise-wide and supports CIMSPA's commitment to high ethical and operational standards in workforce data governance.

2. Scope

This framework applies to all CIMSPA staff, including agency staff, contractors, partners, suppliers, and third parties who process workforce data on behalf of CIMSPA. It addresses data management, security, and compliance concerns integral to CIMSPA's operational and strategic objectives.

By defining clear roles, policies, and standards, this framework ensures that all data users adhere to best practices while contributing to CIMSPA's workforce development objectives.

3. Policy objectives

3.1 Operational efficiency

Enhance content retrieval efficiency

To ensure efficient decision-making, this framework establishes standards for searchability and retrieval of workforce data. By optimising metadata, indexing, and classification, CIMSPA aims to:

- reduce processing costs and downtime by improving access to relevant data
- ensure compliance with legal requirements by maintaining accurate and retrievable records
- support cross-department collaboration by standardising data structures and access protocols.

Protect CIMSPA's reputation

CIMSPA is committed to maintaining stakeholder trust by ensuring transparent, ethical, and accountable data management. This includes:

- demonstrating good faith in data governance practices
- ensuring data accuracy and compliance in workforce reports and insights
- preventing reputational risks by securing sensitive or personal workforce information.

3.2 Compliance and legal assurance

Ensure comprehensive data creation

This framework ensures all workforce data meets legislative and regulatory requirements. To prevent audit failures and potential fines, CIMSPA will:

- maintain accurate, complete, and well-documented records
- ensure transparency in workforce data reporting and compliance assessments
- balance openness with security, ensuring responsible data-sharing practices.

Manage content according to requirements

Data classification policies will prevent over-management of low-risk data while ensuring strict security for sensitive workforce records. By implementing risk-based data governance, CIMSPA aims to optimise compliance and efficiency.

3.3 Business productivity and decision support

Facilitate timely access to data

- CIMSPA will implement data access frameworks that facilitate secure, role-based access to workforce information.
- Workforce data will be standardised and structured to support trend analysis, forecasting and policy development.

Empower business decisions

- Workforce data will be leveraged for evidence-based decision making in training, workforce development, and resource allocation.
- The framework supports AI-driven insights, improving predictive analytics for future workforce trends.

3.4 Data security and records management

Implement robust security controls

CIMSPA will adopt a multi-layered security approach, ensuring:

- end-to-end encryption for sensitive workforce data
- strict authentication and access management
- proactive monitoring and intrusion detection systems.

3.5 Communication

Ensure effective data sharing and governance awareness

- All CIMSPA staff and stakeholders will receive data governance training to promote compliance, security, and ethical data use.
- Data sharing agreements will be standardised, ensuring all partners comply with CIMSPA' governance standards.

4. Guiding principles

CIMSPA's data governance focuses on the following principles.

4.1 Guiding principles overview

Confidentiality, integrity, and availability

Protect the confidentiality, integrity, and availability of Workforce data through restricted access, safeguarding accuracy, and ensuring availability to the correct individuals.

Accuracy and credibility

Implement data validation checks, ensuring all records remain credible, standardised, and reliable for decision making.

Compliance

Adhere to all relevant legal and regulatory requirements.

Continuous improvement

A Data Governance Committee will conduct annual reviews, ensuring the framework remains up to date with emerging best practices and legal requirements.

5. Policy requirements

5.1 Requirements overview

Awareness programme

Introduce a data governance awareness program for all staff, including contractors, to ensure understanding of obligations, standards, guidelines, laws, regulations, and ethical standards.

Protection principles

Protect the confidentiality, integrity, and availability of data.

Data credibility

Ensure that data and records are accurate and trustworthy.

Implementation

Implement relevant data governance policies, procedures, and guidelines.

Monitoring and review

Conduct regular monitoring and reviews, including access and use of data, compliance with policy obligations, management oversight, and risk assessments.

6. Roles and responsibilities

6.1 Data Governance Committee

Composition:

Representatives from Insight, Digital, Finance (if applicable), HR, and external data governance experts.

Responsibilities:

- Oversee the implementation and effectiveness of the data governance framework.
- Define data governance policies and procedures.
- Approve data classification schemes and access control protocols.
- Regularly review and update the framework.

6.2 Workforce data owner

Responsibilities:

- Define data quality standards and metrics.
- Implement data management processes.
- Collaborate on data quality initiatives.
- Ensure alignment with CIMSPA's strategic objectives.

6.3 Workforce data steward

Responsibilities:

- Promote data quality awareness.
- Monitor data quality metrics and identify issues.
- Train personnel on data management best practices.

6.4 Data users

Responsibilities:

- Understand and comply with data governance policies and procedures.
- Exercise responsible data usage practices, adhering to the principles of least privilege.
- Report any data quality or security concerns.

6.5 Board of Directors

Responsibilities:

- Establish objectives and communicate the importance of data governance.
- Conduct regular management reviews and audits.
- Ensure adequate resources for the implementation and maintenance of the data governance framework.

7. Data management policies and procedures

7.2 Data management policies

Data classification and access control:

- Sensitive data will require restricted access and higher security measures.
- Role-based access will ensure least privilege principles are applied.

Data quality standards:

- Define and monitor data quality metrics.
- Implement data cleansing processes.
- Regular data audits will ensure records remain accurate, complete, and relevant.

Data security protocols:

- Implement data encryption, loss prevention, incident response, and secure disposal procedures.

Data retention and disposal:

- Establish data retention periods based on legal and regulatory requirements.
- Outline secure data disposal procedures.

7.3 Related CIMSPA policies

- Information Security Policy
- Privacy Notice
- Data Retention Schedule
- Malpractice and Maladministration of CIMSPA Policy
- CIMSPA Partner Code of Conduct
- CIMSPA Complaints Policy
- CIMSPA Appeals Policy and Procedure

7.4 Non-compliance and enforcement

Non-compliance with this policy or related policies will be considered misconduct. Repeated or material violations may be considered gross misconduct, subject to disciplinary actions as outlined in CIMSPA's Disciplinary Policy and Procedure. This includes potential termination of employment or contracts, legal action, and other corrective measures.

7.5 Data Governance Framework continuous improvement

The data governance improvement plan will identify the detailed requirements necessary to achieve compliance with the main policy objectives. The Observatory Board will monitor progress and report annually to the corporate management team.

Reporting procedures

- Annual report: Includes major initiatives, successes tied to corporate goals, investment and return, and challenges and risks.
- Quarterly updates: Provide interim progress and highlight any immediate issues or successes.

7.6 Management review

The Data Governance Committee will review the Data Governance Framework annually to evaluate its ongoing suitability, adequacy, and effectiveness in meeting CIMSPA's requirements. In the event of a policy breach, an emergency change management procedure will be enacted to resolve the issue promptly.

8. Appendices

8.1 Regulatory requirements and guiding frameworks:

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- UK Data Protection Bill
- Privacy and Electronic Communications Regulations (PECR)
- National Data Strategy (NDS)
- Data Standards Authority (DSA) Guidelines
- Freedom of Information Act 2000
- Equality Act 2010
- Computer Misuse Act 1990
- Health and Social Care Act 2012
- Safeguarding Vulnerable Groups Act 2006
- Sporting regulations and governing bodies
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Children's Act 2004
- Public Records Act 1958

CIMSPA®

Shaping a recognised, valued and inclusive sport and physical activity sector that everyone can be a part of.