



Data Protection Policy

Date published

October 2026

Introduction

As the professional development body for the UK's sport and physical activity sector, CIMSPA is shaping a recognised and respected sector through its work with individual members and partner organisations. In order to carry out its business, CIMSPA must protect personal data and ensure that it understands the rules governing their use of personal data to which they have access to.

Statement

This policy sets out how we seek to protect personal data and ensure that employees understand the rules governing their use of personal data to which they have access in the course of their work. This policy requires employees to ensure that the Person in Charge of Data be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

We hold personal data about our employees, members, partners, suppliers and other individuals for a variety of business purposes.

We need to collect and use certain types of information about employees, member, partners and other individuals who come into contact with the organisation in order to operate. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

This personal information must be dealt with properly, however it is collected, recorded and used, whether on paper, computer, or recorded on other material and there are safeguards in place to ensure this is undertaken in compliance with relevant legislation including:

- Human Rights Act 1998
- UK GDPR
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations 2004 (where applicable)
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Computer Misuse Act 1990

The Person in Charge of Data has overall responsibility for the day-to-day implementation of this policy.

Scope

This policy applies to all employees who must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy with additional policies and guidelines from time to time. Any new or modified policy will be circulated to employees before being adopted.

Approach

Definitions

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, regulatory, payroll and business development purposes. <i>Business purposes include the following:</i> - <i>Compliance with our legal, regulatory and corporate governance obligations and good practice</i> - <i>Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests</i> - <i>Ensuring business policies are adhered to (such as policies covering email and internet use)</i> - <i>Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, due diligence, security vetting, credit scoring and checking</i> - <i>Investigating complaints</i> - <i>Checking references, ensuring safe working practices, monitoring and managing employee access to systems and facilities, administration and assessments</i> - <i>Monitoring employee conduct, disciplinary matters</i> - <i>Marketing of CIMSPA</i> - <i>Improving services</i>
Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, partner contacts, member, suppliers and marketing contacts. <i>Personal data we gather may include individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title and CV.</i>
Sensitive personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non- membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.
Data Transfer	Data Transfer means any movement, transmission, disclosure, copying, sharing or provision of access to Personal Data from one person, organisation, system, device or location to another, whether by electronic, physical or other means. For the purpose of determining the destination and applicable safeguards of a Data Transfer, CIMSPA will

	regard Personal Data as transferred to the location in which it is received and stored, hosted or otherwise held at rest.
--	---

Fair and Lawful processing

We must process personal data fairly and lawfully, ensuring that each data processing activity is justified, documented, and communicated to the data subject where required. Data will only be retained for as long as necessary to fulfil its purpose and then securely disposed of in compliance with our data retention guidelines.

The Person in charge of Data's responsibilities

- Keeping CIMSPA and its board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all employees and those included in this policy
- Answering questions on data protection from employees, board members and other stakeholders
- Responding to individuals such as partners, members and employees who wish to know what data regarding them is being held by CIMSPA
- All subject access request responsibilities
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing.

Responsibilities of the Information Security Manager

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services CIMSPA is considering using to store or process data

The Processing of all Data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities
- In line with our Privacy Notice and data retention schedule

The notice:

- Sets out the purposes for which we hold personal data on members, partners and employees
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that stakeholders have a right of access to the personal data that we hold about them.

Sensitive Personal Data (Special Categories of data)

In most cases where we process sensitive personal data, we will require the data subject's explicit consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and Relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Person in charge of Data.

Your Personal Data

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Person in charge of Data so that they can update your records.

Data Security

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Person in charge of Data will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing Data Securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The Person in charge of Data must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall

Remote working environments must adhere to the same data security standards as on-premises locations. Personal data access from remote locations should be via secure, company-approved networks and devices to prevent unauthorised access.

Data Retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, considering the reasons that the personal data was obtained and should be determined in a manner consistent with our data retention guidelines.

Transferring Data Internationally

There are restrictions on international transfers of personal data. You must not transfer personal data outside the UK or the EEA.

Processing Data in accordance with the Individuals Rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Person in Charge of Data about any such request.

Explicit consent is required for any electronic direct marketing if there is no existing business relationship. Consent must be verifiable, including who, when, and how consent was given, and individuals must be informed on how to

withdraw consent easily. Please contact the Person in Charge of Data for advice on direct marketing before starting any new direct marketing activity.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Training completion will be recorded and tracked by their Manager with oversight by the Person in Charge of Data, ensuring all staff meet training requirements within set timelines. Refresher training sessions will also be conducted annually to reinforce core data protection principles. Training is provided via the Learning Management System (LMS). It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.

Completion of training is compulsory.

Subject Access Requests

Please note that under the Data Protection legislation, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, refer it immediately to the Person in Charge of Data. The Person in Charge of Data will coordinate responses within one month, in accordance with GDPR guidelines. Staff must support SAR processing as requested to meet regulatory deadlines. We may ask you to help us comply with those requests. We cannot charge the data subject for requesting this information however, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

We may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that we can charge for all subsequent access requests. The fee must be based on the administrative cost of providing the information.

Please contact the Person in Charge of Data at compliance@cimspa.co.uk if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

GDPR Provision

Privacy Notice – Transparency of Data Protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. Please read this policy in conjunction with the [CIMSPA Privacy Notice](#).

Privacy by design and default

A Privacy Impact Assessment (PIA) must be conducted for all new data processing activities involving personal data. The Person in Charge of Data will assist in identifying privacy risks and propose necessary controls to mitigate these risks, ensuring compliance and safeguarding individual rights. The Person in Charge of Data will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.

When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

Data Audit and Register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting Breaches

All members of staff must report any actual or suspected data protection compliance failures within 24 hours. The Person in Charge of Data will determine if escalation to the supervisory authority is required within 72 hours and assess the need to inform affected individuals directly.

We only need to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we must notify those concerned directly. A 'high risk' means the threshold for notifying individuals is higher than for notifying the relevant supervisory authority.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both us and our data subjects at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Person in Charge of Data.

Monitoring and Breaches

The Person in Charge of Data has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

All breaches of information, actual or suspected must be reported to the Person in Charge of Data who will ensure they are investigated. Breaches of this policy may be considered as gross misconduct and in certain cases lead to termination of employment and/or legal action/prosecution.

Review of the Privacy Notice

This privacy notice will be kept under review and if amended notification will be made on the CIMSPA website.

Where CIMSPA makes substantial changes or a new use for individual's personal data is identified, it will provide individuals with an updated version of the Data Protection Policy before such changes or new uses take place.