Mindful Peak Performance CIC

Data Protection Policy

Policy Review Date: August 2026
Next Review Date: August 2027
Approved By: Mindful Peak Performance CIC Board of Directors

L Doherty
M Daniel
J Russell

Definitions

Organisation	Mindful Peak Performance CIC (MPP), a Community Interest Company and social enterprise.
UK GDPR	The United Kingdom General Data Protection Regulation, as amended from time to time.
DPA 2018	The Data Protection Act 2018.
DUAA 2025	The Data (Use and Access) Act 2025, which amended UK data protection law and whose data-protection provisions are now in force.
Responsible Person	Luke Doherty, Managing Director, who acts as MPP's Data Protection Lead unless the Board appoints another person.
Personal data	Information relating to an identified or identifiable living person.
Special category data	Personal data requiring additional protection, including data about health, racial or ethnic origin, religious or philosophical beliefs, trade union membership, genetics, biometrics used for identification, sex life or sexual orientation.
Processing	Any operation performed on personal data, including collecting, recording, storing, viewing, sharing, changing or deleting it.
Data subject	The person the personal data relates to.
Register of Processing Activities	MPP's record of the personal data it processes, why it is processed, the lawful basis, who it is shared with, retention periods and relevant safeguards.

1. Introduction

Mindful Peak Performance CIC (MPP) is committed to protecting personal data and respecting the privacy rights of the people we work with. Our work may involve personal data relating to participants, children and young people, adults at risk, parents and carers, staff, volunteers, facilitators, directors, partner organisations, funders, suppliers and other contacts.

This policy explains how MPP will collect, use, store, share and dispose of personal data lawfully, fairly, transparently and securely. It applies to personal data held electronically, on paper, in photographs or recordings, and in any other format.

MPP will comply with the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, the Privacy and Electronic Communications Regulations (PECR) where relevant, and current guidance issued by the Information Commissioner's Office (ICO).

2. Scope and responsibilities

This policy applies to all directors, employees, sessional staff, freelancers, contractors and volunteers who process personal data on behalf of MPP.

- The Board is responsible for oversight of data protection governance and for ensuring appropriate resources and controls are in place.
- The Responsible Person leads on data protection compliance, supports staff, manages data rights requests and complaints, coordinates breach response and keeps this policy under review.
- All staff and volunteers must follow this policy, complete relevant training, use approved systems and report suspected data breaches or poor practice immediately.
- Anyone who knowingly or recklessly misuses personal data may be subject to disciplinary action and, where relevant, legal consequences.

3. Why MPP collects and uses personal data

MPP only collects and uses personal data where there is a clear and legitimate purpose. This may include:

- Delivering BAM! Body and Mind Training and other wellbeing, community and training programmes.
- Registering participants, managing attendance, communication, accessibility and reasonable adjustments.

- Protecting children, young people and adults at risk and meeting safeguarding responsibilities.
- Managing staff, facilitators, volunteers, directors and recruitment processes, including DBS information where lawfully required.
- Managing contracts, invoices, payments, insurance, suppliers and partner relationships.
- Monitoring, evaluating and improving programmes and reporting appropriately to funders and partners.
- Meeting legal, regulatory, accounting, insurance and governance obligations.
- Communicating about MPP services, events and opportunities where lawful, including direct marketing in accordance with PECR.
- Managing enquiries, complaints, incidents, accidents and claims.
- Using photographs, video or testimonials where an appropriate lawful basis and any required permissions are in place.

4. Data protection principles

MPP will apply the seven UK GDPR principles to all processing of personal data:

- Lawfulness, fairness and transparency - personal data will be used lawfully, fairly and in ways people can reasonably understand.
- Purpose limitation - personal data will be collected for specified, explicit and legitimate purposes and will not be reused incompatibly.
- Data minimisation - only personal data that is adequate, relevant and necessary will be collected and used.
- Accuracy - reasonable steps will be taken to keep personal data accurate and up to date.
- Storage limitation - personal data will not be kept in identifiable form for longer than necessary.
- Integrity and confidentiality - appropriate technical and organisational measures will protect personal data from loss, misuse, unauthorised access, alteration or disclosure.
- Accountability - MPP will take responsibility for compliance and keep appropriate records to demonstrate it.

5. Lawful bases for processing

Before processing personal data, MPP will identify and document an appropriate lawful basis. Depending on the activity, this may be:

- Consent
- Contract
- Legal obligation
- Vital interests

- Public task, where applicable
- Recognised legitimate interest, where the statutory conditions are met
- Legitimate interests, following a necessity and balancing assessment where required

Consent will not be used by default where another lawful basis is more appropriate. Where MPP relies on consent, it must be freely given, specific, informed and unambiguous, and it must be as easy to withdraw as to give.

6. Special category and criminal offence data

MPP may process sensitive information in connection with safeguarding, health and wellbeing, equality monitoring, accessibility, recruitment and programme delivery. This may include health information and information revealing racial or ethnic origin, religion, sexual orientation or other special category data.

MPP will only process special category data where both an Article 6 lawful basis and a valid Article 9 condition apply. Where the Data Protection Act 2018 requires an additional Schedule 1 condition or an Appropriate Policy Document, MPP will put this in place before processing.

Criminal offence data, including relevant DBS information, will only be processed where there is a lawful basis and appropriate legal authority or condition. Access will be tightly restricted and information will not be retained longer than necessary.
Equality and diversity information will, wherever practical, be collected in a way that minimises identifiability and will be anonymised or aggregated for reporting.

7. Children and young people

MPP works extensively with children and young people and recognises that their personal data requires particular care. Privacy information will be clear and age appropriate, and data collection will be limited to what is necessary for programme delivery, safeguarding, evaluation and legal obligations.

When designing services, systems or processes likely to be accessed by children, MPP will consider the higher level of protection required for children and apply data protection by design and by default. Safeguarding needs will be balanced with privacy, and information will only be shared where there is a lawful and proportionate reason to do so.

8. Transparency and privacy information

MPP will provide appropriate privacy information when personal data is collected, or within the legally required period where data is obtained from another source. Privacy information will explain, in clear language:

- Who MPP is and how to contact us.
- What personal data is collected and why.
- The lawful basis for processing and, where relevant, legitimate interests.
- Who data may be shared with.
- How long data is kept or how the period is decided.
- Any relevant international transfers and safeguards.
- The individual's data protection rights.
- How to raise a data protection complaint with MPP and how to contact the ICO.
- Where relevant, the use of automated decision-making or profiling.

9. Individual rights

MPP will respect the rights available to individuals under UK data protection law. Depending on the circumstances, these include the rights to be informed, access personal data, rectify inaccurate data, erase data, restrict processing, data portability, object to processing, and rights relating to automated decision-making and profiling.

A request does not need to mention data protection law or be made in writing. Staff who receive a request must forward it to the Responsible Person immediately.

Subject access requests will be handled without undue delay and normally within one month. Where the law permits an extension, clarification, identity check or fee, MPP will communicate this promptly and follow current ICO guidance. Searches will be reasonable and proportionate, and information will be disclosed securely with appropriate consideration of third-party rights and exemptions.

10. Data protection complaints

MPP will maintain a clear process for people to make complaints about how their personal data has been handled. Complaints may be made verbally or in writing and should be passed to the Responsible Person without delay.

MPP will acknowledge a data protection complaint within 30 days unless a full response is provided within that period. The complaint will be investigated appropriately and the outcome communicated without unjustifiable or excessive delay. Records of complaints, investigations and outcomes will be retained as necessary to demonstrate compliance and organisational learning.

Individuals will be informed of their right to complain to the Information Commissioner's Office if they remain dissatisfied.

11. Data minimisation and accuracy

MPP will only collect information that is necessary for the purpose identified. Forms, spreadsheets, monitoring systems and partner reporting requirements should be reviewed to avoid collecting excessive or unnecessary personal data.

Staff should take reasonable steps to keep personal data accurate, particularly contact, safeguarding, payment and employment information. Where an individual tells MPP that data is inaccurate, it will be corrected or appropriately noted without undue delay.

12. Retention, archiving and secure disposal

MPP will maintain and review a retention schedule covering the main categories of records it holds. Retention periods will reflect legal, contractual, safeguarding, insurance, employment, financial and operational requirements.

Personal data must not be retained indefinitely simply because storage is available. At the end of the retention period it will be securely deleted, destroyed, anonymised or reviewed where continued retention is justified.

Paper records containing personal data will be stored securely and disposed of by confidential shredding. Electronic data will be deleted using methods appropriate to the system and risk, including removal from shared drives, devices and accounts where relevant.

13. Data security

MPP will use proportionate technical and organisational measures to protect personal data. These include, where appropriate:

- Using approved, supported software and cloud services and applying security updates promptly.
- Using strong unique passwords and multi-factor authentication wherever available, particularly for email, cloud storage and administrative accounts.
- Limiting access according to role and need-to-know principles and removing access promptly when roles change or people leave.

- Protecting laptops, phones and other devices with passcodes, encryption and automatic locking where available.
- Keeping confidential paper records locked away when not in use.
- Using secure methods for transferring sensitive information and checking recipients before sending emails or attachments.
- Avoiding storage of personal data on personal devices, unapproved apps or personal cloud accounts unless specifically authorised and appropriately secured.
- Using backups and recovery arrangements proportionate to the importance of the data.
- Being alert to phishing, social engineering and accidental disclosure and reporting concerns immediately.
- Keeping safeguarding and other particularly sensitive records separated or access-restricted where practical.

14. Working remotely, mobile devices and messaging

The same data protection standards apply when working remotely, travelling or delivering sessions in community settings. Staff and facilitators must take reasonable steps to prevent conversations, screens, paperwork or devices being seen or accessed by unauthorised people.

Personal data should only be shared through approved communication channels. Messaging applications may only be used where MPP has approved their use for the specific purpose and appropriate security, retention and safeguarding arrangements are in place.

15. Sharing personal data

MPP may share personal data with partner organisations, commissioners, funders, safeguarding agencies, professional advisers, service providers or public authorities where there is a lawful and proportionate reason to do so.

Before sharing personal data, staff should consider what needs to be shared, with whom, why, under what lawful basis, and how it can be transferred securely. Data should be anonymised or aggregated where identifiable information is not required.

Safeguarding information may be shared without consent where this is necessary and lawful to protect a child, young person or adult at risk or to meet another legal obligation. Decisions should be documented and follow MPP safeguarding procedures.

16. Processors, contracts and third-party systems

Where another organisation processes personal data on MPP's behalf, MPP will carry out proportionate due diligence and ensure an appropriate written data processing contract is in place. Contracts will address confidentiality, security, instructions, sub-processors, assistance with rights requests and breaches, deletion or return of data, and audit or assurance requirements as appropriate.

New software or online platforms should not be adopted for storing personal data without considering privacy, security, data location, access controls, retention and supplier terms.

17. International data transfers

MPP will not transfer personal data outside the UK unless the transfer is lawful. Where an adequacy regulation does not apply, MPP will use an appropriate safeguard such as the UK International Data Transfer Agreement, UK Addendum or another legally permitted mechanism, together with any required transfer risk assessment.

18. Data protection by design, DPIAs and new projects

Privacy and data protection will be considered at the start of new programmes, partnerships, technologies, forms and methods of evaluation rather than added afterwards. A Data Protection Impact Assessment (DPIA) will be completed before processing that is likely to result in a high risk to individuals. This may include significant new uses of sensitive data, large-scale monitoring, novel technology, systematic profiling, or other high-risk processing. The Responsible Person should be consulted where staff are unsure whether a DPIA is required.

19. Automated decision-making and artificial intelligence

MPP will not use solely automated decision-making that produces legal or similarly significant effects on individuals unless a lawful basis and all required safeguards are in place. Any use of artificial intelligence tools involving personal data must be approved, proportionate and consistent with this policy.

Staff must not enter confidential, safeguarding, health, participant, employee or other identifiable personal data into public or unapproved AI services. Where AI tools are

approved, MPP will consider data protection by design, transparency, accuracy, security, human oversight, supplier terms and retention.

20. Direct marketing, email and cookies

Marketing communications will comply with data protection law and PECR. Where consent is required, MPP will use a clear opt-in and keep evidence of consent. Every direct marketing communication will provide a simple way to opt out, and suppression records may be retained where necessary to ensure people who opt out are not contacted again.
MPP's website will provide appropriate information about cookies and similar technologies and will seek consent where required by PECR. Non-essential cookies will not be set before any required consent is obtained.

21. Personal data breaches

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. Examples include sending information to the wrong recipient, losing a device or paper file, compromised passwords, unauthorised access, malware, or accidental publication.

All suspected breaches must be reported immediately to the Responsible Person. Staff must not delay reporting while investigating the incident themselves.

MPP will contain and investigate the breach, record the facts and decisions, assess the risk to people's rights and freedoms and take action to reduce harm. Where a breach is likely to result in a risk to people's rights and freedoms, MPP will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it. Where the risk is high, affected individuals will also be informed without undue delay unless an exemption applies.

22. Records, training and accountability

MPP will maintain appropriate records of processing activities, lawful bases, privacy information, data sharing, processor arrangements, retention decisions, DPIAs, rights requests, complaints and personal data breaches.

All staff and volunteers who handle personal data will receive appropriate data protection and information security guidance or training as part of induction and periodic refreshers.

Additional training will be provided where roles involve safeguarding, special category data, recruitment or other higher-risk processing.

23. Data Protection Lead and contact details

Responsible Person / Data Protection Lead

Luke Doherty
Managing Director
Mindful Peak Performance CIC
Email: luke@mindfulpeakperformance.com
Phone: 07787 436889

Data protection concerns, rights requests and complaints should be sent to the Responsible Person using the contact details above. Individuals may also contact the Information Commissioner's Office (ICO) if they have concerns about the use of their personal data.

24. Policy review and approval

This policy will be reviewed at least annually and sooner where there are significant changes in law, ICO guidance, MPP's activities, technology, data processing or organisational risk.

Relevant legislation and guidance

- UK General Data Protection Regulation (UK GDPR), as amended
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), as amended
- Information Commissioner's Office guidance, including current guidance on data protection principles, individual rights, data protection complaints, security, data protection by design and special category data