Data Protection Policy

Policy owner: Michael Howe – Deputy CEO
Policy lead: Peter Fisher, Associate Director of Legal and Governance
Trustee committee responsible: Audit & Risk
Formally endorsed: July 2021

Last updated: April 2026
Next Review: April 2027

Policy statement
One YMCA Limited ('One YMCA', 'we', 'us', and 'our') is committed to respecting and protecting the privacy of individuals and to fully complying with all the requirements of Data Protection Legislation.

We have appointed an internal Data Protection Officer (DPO) who can be contacted via data.protection@oneymca.org please direct any initial data protection queries or concerns to the DPO in the first instance.

You can contact the Information Commissioner's Office via their helpline on 0303 123 1113 or by submitting an enquiry through their website using this link

SCOPE

This policy applies to all our staff.

This policy, which is part of our suite of data protection related policies, must be followed in conjunction with those other policies.

This policy applies to all of our business activities that involve the processing of personal data.

ASSOCIATED POLICIES & RELATED DOCUMENTS

This policy must be read in conjunction with the following:

- Information Security Policy
- Data Retention Policy
- Privacy Notices (Organisation-wide and service-specific)
- Subject Access Request Procedure
- ICT Acceptable Use Policy
- Breach Response Procedure (within this policy)

DEFINITIONS

Data Protection Legislation means the UK General Data Protection Regulation, ('UK GDPR'), the Privacy and Electronic Communications Regulations ('PECR') and (where applicable) the EU General Data Protection Regulation ('EU GDPR').

Personal data (aka Personal Information and Personally Identifiable Information or PII) means any information relating to an identified or identifiable person ('Data Subject').

Personal data breach means a security incident that has affected the confidentiality, integrity, or availability of personal data (whether accidental or deliberate).

Examples of personal data typically processed by us are:

- First and last names
- Postal email and IP addresses
- Telephone numbers
- Identity documents (e.g., passports & driving licence)
- Identity numbers (e.g., National Insurance and Bank accounts)
- Career & educational documents (e.g., CVs & qualifications)
- Any contact information

Special Category data (*aka Sensitive Data*) means personal data revealing racial or ethnic origin, political opinions, religious (including religious-related dietary preferences) or philosophical beliefs, trade-union membership, genetic information of a living individual; biometric data processed solely to identify a living individual; health-related data (including allergies, intolerances, hospitalisations, adverse reactions to products or substances); data concerning a person's sex life or sexual orientation.

Examples of special category personal data typically processed by us are:

- Health & medical information (including whether a person has a disability)
- Info. about ethnic origin & race
- Staff sickness records

Criminal Offence Data: Criminal offence data refers to information relating to criminal convictions and offences or related security measures. This includes allegations, proceedings, and outcomes of criminal activity. We will only process such data where it is strictly necessary, and in accordance with Article 10 of the UK GDPR and Schedule 1 of the Data Protection Act 2018, ensuring appropriate safeguards are in place.

Data subject means any individual whose personal data is processed by us.

Examples of our data subjects are:

- Clients/customers
- Staff and their next of kin
- Job applicants
- Suppliers of goods/service
- Business contacts

Processing means any use of personal data such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination, erasure and destruction. (This means that virtually anything we do with personal data will be 'processing').

Data controller means the organisation which decides the purposes and means of the processing of personal data. We are the data controller for the purposes of this policy.

Data processor means an individual or organisation that processes personal data on behalf of a data controller (on our behalf/on our instructions).

Examples of data processors are:

- External payroll
- External IT support
- Service delivery Partners

Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Staff means **anyone working at or for** us including:

- Board members
- Directors
- Permanent, interim, and temporary employees and workers
- Consultants
- Contractors

PURPOSES

- To ensure all personal data is processed in accordance with Data Protection Legislation
- To respect the privacy of individuals
- To ensure personal data is processed by us in a consistent manner
- To reduce the risk of a personal data breach
- To provide guidance to staff about how to comply with Data Protection Legislation
- To clarify responsibilities and roles for implementing this policy and monitoring compliance with it.

DATA PROTECTION PRINCIPLES AND GOVERNANCE

We are committed to upholding the highest standards of data protection across all processing activities. In doing so, we endorse and adhere to the following core principles, as set out in Article 5 of the UK GDPR, ensuring that personal data is:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes and not further processed in a way that is incompatible with those purposes ('purpose limitation')
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ('data minimisation')
4. Accurate and, where necessary, kept up to date ('accuracy')
5. Kept for no longer than is necessary ('storage limitation')
6. Processed securely, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing, and against accidental loss, destruction, or damage ('integrity and confidentiality')

In line with these principles, we maintain robust governance and documentation measures to support accountability and transparency, including:

- A comprehensive Record of Processing Activities (ROPA) that details the purposes, lawful bases, and categories of personal data processed
- Documented Data Sharing Agreements (DSAs) and clear protocols for any third-party data disclosures
- A defined Data Retention Policy and Data Map outlining how long personal data is kept and how retention is monitored and reviewed
- Regular reviews of data processing practices, training, and oversight to ensure continued compliance and good data governance

RISK APPETITE IN STATUTORY COMPLIANCE

Our organisation maintains a low-risk appetite in all matters relating to statutory and regulatory compliance. We are committed to fully complying with all applicable laws, regulations, and official guidance to uphold the highest standards of legal and ethical conduct.
We adopt a risk-averse approach when processing personal data and ensuring regulatory obligations are met, particularly in areas where non-compliance could result in legal penalties, reputational damage, or harm to data subjects. This includes, but is not limited to:

- Adhering to the UK GDPR and Data Protection Act 2018
- Observing sector-specific statutory requirements
- Complying with obligations related to data subject rights, data security, and breach notification

We continuously review our compliance framework and implement internal controls, audits, and staff training to identify and mitigate risks at the earliest possible stage.

ROLES AND RESPONSIBILITIES

Our Trustees have ultimate responsibility for ensuring compliance with Data Protection Legislation and this policy.

The Data Protection Officer (DPO), has responsibility to

- Remind the Trustees of their responsibility for ensuring our compliance with Data Protection Legislation and this policy; and
- Advise the Trustees how to exercise their responsibility for ensuring our compliance with Data Protection Legislation and this policy; and
- Monitor our compliance with Data Protection Legislation and this policy

Our Data Protection Group (see Appendix) has responsibility to liaise with the DPO to help ensure we comply with the Data Protection Legislation and this policy.

All staff have a responsibility to comply with Data Protection Legislation and this policy when carrying out their duties.

Line managers are responsible for ensuring staff's adherence with this policy.

Failure to comply with this policy or with Data Protection Legislation may result in disciplinary action up to and including dismissal.

In serious cases, individuals may also face:

- criminal prosecution under the UK GDPR or the Data Protection Act 2018;
- civil liability, including compensation claims from affected individuals.

All staff are required to follow the policies and procedures set out in this document and related policies.

RIGHTS

Data subjects have the right to:

1. **Be informed** about the collection and use of their personal data this is a key transparency requirement under the UK GDPR, ensuring individuals are made aware of how and why their personal data is processed. Full details of our data practices, including the lawful bases for processing, types of data collected, and individuals' rights, are outlined in our Privacy Notice.
2. **Access** their personal data (for more about this see 'Subject Access Requests', below)
3. **Rectification** of inaccurate personal data
4. **Erasure** (deletion) of their personal data (also known as the 'right to be forgotten) *

5. **Restrict processing** of their personal data*
6. **Data portability -** to easily move, copy or transfer their personal data
7. **Object** to processing (in certain circumstances)
8. **Appropriate decision-making** in relation to automated decision making and profiling

*This is not an absolute right and only applies in certain circumstances

LAWFUL BASES

We must always have a valid lawful basis in order to process personal data.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on our purpose and relationship with the data subject.

The lawful bases for processing are:

- **Consen**t: the data subject has given clear consent for you to process their personal data for a specific purpose.
- **Contract**: the processing is necessary for a contract we have with the data subject, or because they have asked us to take specific steps before entering into a contract.
- **Legal obligation**: the processing is necessary for us to comply with the law.
- **Vital interests**: the processing is necessary to protect someone's life.
- **Public task***: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- **Legitimate interests**: the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

*This lawful basis is only available to public authorities or bodies.

SUBJECT ACCESS REQUESTS

Any data subject may make a Subject Access Request, ('SAR'). Any one member of staff in receipt of a SAR must pass it on to our Data Protection Group as soon as possible, as a matter of urgency.

SECURITY

All staff are responsible for ensuring that any personal data which we are responsible for is kept securely.

Examples of keeping personal data secure are:

- Paper files/records should be kept in locked cabinets when not in use
- Monitors/computer screens should be visible only to those who need to see them
- Paper files/records should not be removed from our business premises without appropriate authorisation
- Desks should be cleared when not in use
- Personal data no longer required for day-to-day use should be sent to secure archiving

SHARING (DISCLOSURE)

Personal data must not be shared unless the recipient is authorised to have access to that personal data and then only in accordance with Data Protection Legislation.

This includes the sharing of personal data by Staff with

- other members of staff; and
- third parties (other organisations and individuals - including our data processors)

Examples of unauthorised recipients are:

- Family members
- Friends

- Local Authorities and other public bodies

Staff should exercise great caution when asked to share personal data and if in doubt should seek advice from our Data Protection Group before doing so. All decisions to share personal data must be recorded.

Staff should not share any Special Category data (see above) without obtaining advice from our Data Protection Group.

RETENTION

Personal data must not be kept for any longer than is necessary and only in accordance with our Retention Policy.

DELETION (DISPOSAL)

When it is no longer necessary to keep it, personal data must be disposed of securely.

This means that:

- Paper will be shredded on site, or disposed of externally as confidential waste
- Computer equipment will be disposed of securely by specialist contractors

TRANSFER OUTSIDE THE EEA

The UK GDPR restricts the transfer (sending) of personal data outside the UK. This means that personal data cannot be freely transferred outside the UK, except to the EEA and a limited number of other countries.

You should not agree to transfer personal data outside the UK unless you are authorised to do so. If in doubt contact our Data Protection Group.

DATA PROTECTION IMPACT ASSESSMENTS

A data protection impact assessment (DPIA) is a process to help identify and minimise the data protection risks of a project.

We must do a DPIA for processing that is likely to result in a high risk to individuals. This includes some specified types of processing. It is also good practice to do a DPIA for any other new project which requires the processing of personal data.

Any circumstances where a DPIA may be required should not be undertaken without the approval of our Data Protection Group.

MARKETING

The PECR (see definition 'Data Protection Legislation' above), give people specific privacy rights in relation to electronic communications. There are specific rules on:

- marketing calls, emails and texts
- cookies (and similar technologies)

These rules mean that:

- We must not send marketing messages/materials to those who are 'consumers' without being sure that they have previously agreed (consented) to being sent them, do not object to hearing from us and, that by contacting them, we are not being a nuisance to them.
- We must tell people if we set cookies on our website and clearly explain what the cookies do and why. We must also (usually) also get the user's consent to set cookies.

DATA BREACH NOTIFICATION

One YMCA treats all personal data breaches with the utmost seriousness. Upon becoming aware of a breach, we will carry out an immediate internal assessment to determine the likelihood and severity of risk to individuals.

If required, we will notify the ICO within 72 hours, and notify affected individuals without undue delay where a high risk exists. All breaches, whether reportable or not, will be recorded in our internal Breach Log along with assessments and remedial actions taken.

When a personal data breach is suspected or confirmed, One YMCA will follow the structured internal procedure below:

- **Identify & Contain**

All staff must report any actual or suspected personal data breach to the Data Protection Group and the DPO *immediately* and within the same working day.

- **Assess the Risk to Individuals**

The DPO will carry out a formal risk assessment to determine:

- the likelihood of harm to individuals;
- the severity of potential impact;
- whether the breach is likely to result in a **risk** or **high risk** to the rights and freedoms of individuals.

This assessment will be recorded in the Breach Log.

- **Notify the ICO (where required)**

If the breach is assessed as posing a risk to individuals' rights and freedoms, One YMCA will notify the ICO **within 72 hours** of becoming aware of the breach, even if full details are not yet available.

The notification will include:

- the nature of the breach;
- categories and approximate number of data subjects and records affected;
- likely consequences;
- measures taken or proposed to address the breach;
- contact details of the DPO;
- any mitigation actions.

- **4. Notify Affected Individuals**

Where a breach is likely to result in a **high risk** to individuals' rights and freedoms, affected individuals will be notified **without undue delay**.
Notifications will explain:

- the nature of the breach;
- likely consequences;
- what we have done to address it;
- recommended steps individuals should take to protect themselves (e.g., password changes, alerting banks, fraud watch);
- DPO contact details.

5. Documentation & Retention
All breaches — whether reportable or not — will be documented in a secure **Personal Data Breach Log**, including:

- facts relating to the breach;
- its effects;
- remedial actions taken;
- decisions regarding notification (including rationale).

These records will be retained in accordance with the Retention Policy.

Appendix

At the time this policy was last updated, the members of our Data Protection Group were:

1. Peter Fisher (peter.fisher@oneymca.org)
2. Michael Howe (michael.howe@oneymca.org)
3. Deanna Coe (deanna.coe@oneymca.org)
4. Elnaz Farab (Elnaz.farab@oneymca.org)

This policy was last updated on 30.06.2025

Version History:

Last Updated:	Next Review:	Changes:
April 2024	April 2025	Initial issue
June 2025	June 2026	Audit actions
April 2026	April 2026	Add breach procedure, disciplinary details, training, associated policies