

Data Protection Policy

Introduction and Policy Statement

The Trustees and management the of YMCA Plymouth, located at Honicknowle Lane, Honicknowle, Plymouth are committed to compliance with all relevant UK and EU laws in respect of personal data, and the protection of the “rights and freedoms” of individuals whose information The Association collects and processes in accordance with the Data Protection Act 2018.

Compliance with the Act is described by this policy and other relevant policies, along with connected processes and procedures.

Information is a strategic asset of YMCA Plymouth that must be managed accordingly.

In order to operate efficiently, YMCA Plymouth has to collect and use information about people with whom it works and for whom it provides services. These include members of the public, current, past and prospective employees, clients customers, and suppliers. The Association is also required to collect and process information in order to comply with specific legislation.

The policy ensures that YMCA Plymouth complies with the Data Protection Act 2018 and all of the provisions in that act, which implement the EUs General Data Protection Regulation (GDPR) into UK law.

This policy applies to all Departments, Partners, Employees and contractual third parties and agents of YMCA Plymouth.

It is the responsibility of managers within departments to exercise appropriate controls to minimise the risk of breach of this policy.

Anyone found to be in breach of this policy may be subject to disciplinary policies.

Partners and any third parties working with or for the Association, and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy. No third party may access personal data held by The Association without having first entered into a data confidentiality agreement, which imposes on the third party obligations no less onerous than those to which the Association is committed, and which gives the Association the right to audit compliance with the agreement.

Responsibilities and roles under the Data Protection Act

The Association is a data controller / data processor under the Act.

Senior Management and all those in managerial or supervisory roles throughout The Association are responsible for developing and encouraging good information

handling practices within The Association; responsibilities are set out in individual job descriptions.

The Data Protection Lead, will work alongside the Leadership team and be accountable to Trustees of the Association for the management of personal data within The Association and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes: development and implementation of the Data Protection Act as required by this policy; and risk management in relation to compliance with the policy.

The Data Protection Lead, who the Trustees considers to be suitably qualified and experienced, has been appointed to take responsibility for the Association's compliance with this policy on a day-to-day basis and, in particular, has direct responsibility for ensuring that the Association complies with the Act, as do all Managers in respect of data processing that takes place within their area of responsibility.

The Data Protection Lead has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and are the first point of call for Employees seeking clarification on any aspect of data protection compliance.

Compliance with data protection legislation is the responsibility of all Employees of The Association who process personal data.

The association's Data Protection Training Policy sets out specific training and awareness requirements in relation to specific roles and Employees of The Association generally.

Employees of the Association are responsible for ensuring that any personal data about them and supplied by them to The Association is accurate and up-to-date.

Data protection principles

All processing of personal data must be conducted in accordance with the data protection principles as set out in the Data Protection Act. The Association's policies and procedures are designed to ensure compliance with the principles.

Personal data must be processed lawfully, fairly and transparently

Lawful – identify a lawful basis before you can process personal data. These are often referred to as the “conditions for processing”, for example consent.

Fairly- in order for processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data was obtained directly from the data subjects or from other sources.

The Act has increased requirements about what information should be available to data subjects, which is covered in the ‘Transparency’ requirement.

Transparently – the Act includes rules on giving privacy information to data subjects. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must, as a minimum, include:

- the identity and the contact details of the controller and, if any, of the controller's representative;
- the contact details of the Data Protection Lead;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the period for which the personal data will be stored;
- the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;
- the categories of personal data concerned;
- the recipients or categories of recipients of the personal data, where applicable;
- where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;
- any further information necessary to guarantee fair processing.

Personal data can only be collected for specific, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose and must not be processed in a manner that is incompatible with those purposes.

Personal data must be adequate, relevant and limited to what is necessary for processing.

The Data Protection Lead is responsible for ensuring that The Association does not collect information that is not strictly necessary for the purpose for which it is obtained.

All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement and approved by the Data Protection Lead.

The Data Protection Lead will ensure that, on an annual basis all data collection methods are reviewed to ensure that collected data continues to be adequate, relevant and not excessive

Personal data must be accurate and kept up to date with every effort to erase or rectify without delay

Data that is stored by the data controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

The Data Protection Lead is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

It is also the responsibility of the data subject to ensure that data held by The Association is accurate and up to date. Completion of a registration or application form by a data subject will include a statement that the data contained therein is accurate at the date of submission.

Employees/Staff/customers/suppliers should be required to notify The Association of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of The Association to ensure that any notification regarding change of circumstances is recorded and acted upon.

The Data Protection Lead is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

On at least an annual basis, the Data Protection Lead will review the retention dates of all the personal data processed by The Company, by reference to the data inventory, and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed.

The Data Protection Lead is responsible for responding to requests for rectification from data subjects within one month (Subject Access Request Procedure). This can be extended to a further two months for complex requests. If The Association decides not to comply with the request, the Data Protection Lead must respond to the data subject to explain its reasoning and inform them of their right to complain to the supervisory authority and seek judicial remedy.

The Data Protection Lead is responsible for making appropriate arrangements that, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the personal data to the third party where this is required.

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Where personal data is retained beyond the processing date, it will be *[minimised/encrypted/pseudonymised]* in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the Retention of Records Procedure and, once its retention date is passed, it must be securely destroyed as set out in this procedure.

The Data Protection Lead Owner must specifically approve any data retention that exceeds the retention periods, and must ensure that the justification is clearly identified. This must be written.

Personal data must be processed in a manner that ensures the appropriate security. The Data Protection Lead will carry out a risk assessment taking into account all the circumstances of The Association's controlling or processing operations.

In determining appropriateness, the Data Protection Lead should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on the Association itself, and any likely reputational damage including the possible loss of customer trust.

When assessing appropriate technical measures, the Data Protection Lead will consider the following:

- Password protection
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media
- Virus checking software and firewalls
- Role-based access rights including those assigned to temporary staff.
- Encryption of devices that leave the organisations premises such as laptops;
- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to the Association.

When assessing appropriate organisational measures the Data Protection Lead will consider the following:

- The appropriate training levels throughout The Association;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Restricting the use of employee's own personal devices being used in the workplace; and adhering to the company Bring your own Device policy (if applicable)
- Adopting clear rules about passwords;
- Making regular backups of personal data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA.

These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

The Association will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs, breach notification procedures.

Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed.
- To prevent processing likely to cause damage or distress.
- To prevent processing for purposes of direct marketing.
- To be informed about the mechanics of automated decision-taking process that will significantly affect them.
- To not have significant decisions that will affect them taken solely by automated process.
- To sue for compensation if they suffer damage by any contravention of the Act.
- To take action to rectify, block, erased, including the right to be forgotten, or destroy inaccurate data.
- To request the supervisory authority to assess whether any provision of the Act has been contravened.
- To have personal data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- To object to any automated profiling that is occurring without consent.

The Association ensures that data subjects may exercise these rights:

Data subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how The Company will ensure that its response to the data access request complies with the requirements of the Act.

Data subjects have the right to complain to The Association related to the processing of their personal data, the handling of a request from a data subject and appeals from a data subject on how complaints have been handled in line with the Complaints Procedure.

Consent

The Association understands 'consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the data subject's wishes that, by statement or by a clear affirmative action, signifies

agreement to the processing of personal data relating to him or her. The data subject can withdraw their consent at any time.

The Association understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

There must be some active communication between the parties to demonstrate active consent. Consent cannot be inferred from non-response to a communication.

The Controller must be able to demonstrate that consent was obtained for the processing operation.

For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

In most instances, consent to process personal and sensitive data is obtained routinely by The Association using standard consent documents *[reference]* e.g. when a new client signs a contract, or during induction for participants on programmes.

Where The Association provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16.

Security of data

All Employees are responsible for ensuring that any personal data that The Association holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by The Association to receive that information and has entered into a confidentiality agreement

All personal data should be accessible only to those who need to use it. Data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or
- in a locked drawer or filing cabinet; and/or
- if computerised, password protected and/or
- stored on (removable) computer media which are encrypted.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees of the Association.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

Personal data may only be deleted or disposed of in line with the Retention of Records Policy and Procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed before disposal. Processing of personal data 'off-site' presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site

To protect sensitive data through email, all YMCA Plymouth email communications use TLS (Transport Layer Security) encryption from Google Cloud.

Disclosure of data

The Association must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of The Association's business.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Lead.

Retention and disposal of data

The Association shall not keep personal data in a form that permits identification of data subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

The Association may store data for longer periods if the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

The retention period for each category of personal data will be set out in the Retention of Records Procedure along with the criteria used to determine this period including any statutory obligations. The Association has to retain the data. Personal data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

Record of processing activities

The Association has established a data inventory and data flow process as part of its approach to address risks and opportunities throughout its data protection compliance project. The Association's data inventory and data flow determines:

- business processes that use personal data;
- source of personal data;

- volume of data subjects;
- description of each item of personal data;
- processing activity;
- maintains the inventory of data categories of personal data processed;
- documents the purpose(s) for which each category of personal data is used;
- recipients, and potential recipients, of the personal data;
- the role of the Association throughout the data flow;
- key systems and repositories;
- any data transfers and
- all retention and disposal requirements.

The Association is aware of any risks associated with the processing of particular types of personal data.

The Association assesses the level of risk to individuals associated with the processing of their personal data. Data protection impact assessments (DPIAs) are carried out in relation to the processing of personal data by The Association, and in relation to processing undertaken by other organisations on behalf of The Association.

The Association shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this policy.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, The Association shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of personal data. A single DPIA may address a set of similar processing operations that present similar high risks.

Where, as a result of a DPIA it is clear that The Association is about to commence processing of personal data that could cause damage and/or distress to the data subjects, the decision as to whether or not The Association may proceed must be escalated for review to the Data Protection Lead.

The Data Protection Lead shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by and the requirements of the Act.

Communications

A current version of this document is available to all members of staff and volunteers on the Association's Intranet

All staff undertake formal training on Data Protection during their induction period.

All volunteers are briefed on Data Protection during their induction period

Customers and clients have access to our Privacy Policy and Data Protection Policy via links on our website
Students have access to the Data Protection Policy via a dedicated website.

Monitor and Review

Regular reviews of YMCA Policies and Procedures will be undertaken annually. This will be carried out by the Human Resources Business Partner and reported on to the Board of Trustees.

This policy is supplemented by additional guidance as follows:

Training Policy
Bring your own device to work policy
Data Retention Policy
Subject Access Request Policy
Privacy Policy
CCTV Policy

These policies are available on the staff intranet.