Data Protection Policy

Policy owner: Michael Howe – Director of Central Services, Quality & impact
Policy lead: Katie Sandys-Renton – Head of Legal Services
Trustee committee responsible: Audit & Risk
Formally endorsed: July 2021

Last updated: September 2022 – Addition of Signpost CIO, updating of job titles, no other required changes
Next Review: September 2023

Policy statement
One YMCA ('the Charity', 'we', 'us', and 'our') supports people across Hertfordshire, Bedfordshire and Buckinghamshire through a range of crucial services across multiple communities.

We are committed to fully complying with all the requirements of the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR) and all other applicable data protection laws (together 'the data protection legislation').

Scope
This policy applies to the whole of the One YMCA group including the Early Childhood partnership, Signpost CIO and other subsidiaries. Reference to One YMCA ('the Charity', 'we', 'us', and 'our') refers to the parent company and all subsidiaries.

This policy explains how we will comply with our responsibilities and obligations under the data protection legislation and applies to all our staff. It should be read and used in conjunction with our other data protection related policies:

- Privacy
- Retention
- Remote working
- Information Security

Objective
The objective of this policy is to:

- Ensure we follow the principles of data protection as set out in the UK GDPR.
- Ensure personal data is processed in a consistent manner throughout the Charity at all times
- Clarify responsibilities for implementing, complying and monitoring this policy
- Give guidance to staff about what they and the Charity must do to comply with the data protection legislation.

Definitions

Personal data means any information relating to an identified or identifiable living individual.
Examples of personal data typically processed by us are:

- First and last names
- Postal and email 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)
- Contact information
- Children

Special categories of personal data mean personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation and data concerning criminal convictions or offences

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

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

Examples of our data subjects are:

- Service Users
- Staff
- Volunteers
- Trustees
- Donors
- Supporters
- Enquirers and complainants
- Residents
- Members
- Centre users
- People hiring our premises,
- Staff next of kin
- Job applicants
- Suppliers of goods/services
- Business and other contacts
- Anyone whose image is captured by our CCTV

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.

NB: 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

NB: 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

Examples of our data processors are:

- External payroll
- External IT support
- Service delivery Partners

Personal data breach means a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

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:

- Trustees
- Directors
- Permanent, interim and temporary employees
- Volunteers

The principles of data protection
Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are 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 in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')

Roles and responsibilities
Our Trustees have ultimate responsibility for ensuring compliance with the, the data protection legislation, the principles of data protection and this policy.

The Directors have a responsibility for ensuring compliance with the data protection legislation, the principles of data protection and this policy.

The Data Protection Officer (DPO) has a responsibility to remind the Trustees and the Directors of their responsibility for ensuring compliance with the data protection legislation, the principles of data protection and this policy.

The DPO is Robert Wassall of NormCyber Limited. He can be contacted at robert.wassall@normcyber.com.

The Director of Central Services, Quality & Impact has day-to-day operational responsibility for ensuring we comply with the data protection legislation, the principles of data protection and this policy.

All staff have a responsibility to comply with the data protection legislation, the principles of data protection and this policy when carrying out their duties.

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

Failure to comply with this policy may result in legal and/or disciplinary action.

Rights
People have the following rights under the data protection legislation:

1. The right to be informed
2. The right of access*
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

*****Any data subject may make a Subject Access Request, ('SAR') to the Charity. Any member of staff in receipt of a SAR must pass it on to their line manager 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
When considering sharing data, all members of staff must consider the data protection legislation. There are no rules that personal data cannot or must not be shared – only that any sharing is done in compliance with the data protection legislation
This includes the sharing of personal data by Staff with:

- Other members of staff; and
- Third parties/other organisations (including our data processors)

Personal data must not be shared unless the recipient is entitled and authorised to have access to that data.

The following list includes common reasons that the Charity will normally disclose personal data to a third party:

- To give a confidential reference relating to a current or former member of Staff;
- For the prevention or detection of crime;
- For the assessment of any tax or duty (or statutory benefit or equivalent);
- Where it is necessary to exercise a right or obligation conferred or imposed by law upon us (other than an obligation imposed by contract);

- Where it is necessary in relation to duties of safeguarding and the care and/or wellbeing of individuals (this includes obtaining medical references and/or opinions where required for employment matters);
- Where it is necessary for the delivery of services and where the Charity is either the service delivery commissioner, Contractor or Sub-Contractor and there is an appropriate contract and/or data processing agreement in place.

Staff should always exercise great caution when asked to share personal data and if in doubt should seek advice from their line manager (who may liaise with the Director of Corporate Services) before doing so.

All decisions to share personal data must be recorded.

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

Disposal (destruction/deletion)
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

International/cross-border transfers
The data protection legislation generally prohibits the transfer (sending) of personal data outside the European Economic Area (EEA). These restrictions mean that personal data cannot be freely transferred outside the EEA.

All decisions to transfer personal data outside the EEA must be specifically authorised the Director of Corporate Services.

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.

The data protection legislation includes an obligation to conduct a DPIA for types of processing and is good practice to conduct a DPIA for any major 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 your line manager (who may liaise with the Director of Central Services, Quality & Impact).

NB: The responsibilities of the Director of Central Services, Quality & Impact will be largely delivered by the Head of Legal Services and Compliance.