YMCA
NORTH TYNESIDE

Privacy Notice for Job Applicants

Author:	Lynsey Crossman
Checked by relevant people with appropriate expertise and responsibility:	CIPD HR Inform, Lynsey Crossman, Policy Working Group
Approved by:	Steve Pugh
Approval Date:	18/02/2026
Version No:	2
Review date:	Feb 2027

Table of Contents

1. Purpose
2. Scope
3. Definitions
4. Roles and Responsibilities
5. Main Body of Policy
    - 5.1 Data Protection Principles
    - 5.2 Types of Data Held
    - 5.3 Methods of Collection
    - 5.4 Lawful Basis for Processing
    - 5.5 Special Categories of Data
    - 5.6 Criminal Conviction Data
    - 5.7 Data Sharing and Third Parties
    - 5.8 International Transfers
    - 5.9 Retention Periods
    - 5.10 Automated Decision Making
    - 5.11 Individual Rights
6. Related Policies
7. Relevant UK Legislation
8. Monitoring and Review
9. Appendix

1. Purpose

The purpose of this policy is to inform prospective employees, workers, and volunteers of YMCA North Tyneside (The Organisation) about the types of personal data processed during the recruitment and selection process. This document ensures compliance with the UK General Data Protection Regulation (UK GDPR) and provides transparency regarding the reasons for processing data, the lawful basis for doing so, retention periods, and the rights of individuals.

2. Scope

This policy applies to all individuals applying for roles within YMCA North Tyneside, including prospective employees, workers, contractors, and volunteers. It covers the period from the initial application or expression of interest up to the point of employment or rejection.

3. Definitions

- The Organisation: YMCA North Tyneside.
- Personal Data: Any information about an individual from which that person can be identified. This does not include anonymous data.
- Special Category Data: Data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, health data, and data concerning a person's sex life or sexual orientation.
- Processing: Any operation performed on personal data, such as collection, recording, storage, adaptation, use, disclosure, or erasure.
- Applicant: Any individual applying for a position (paid or unpaid) within the Organisation.

4. Roles and Responsibilities

- Data Protection Lead: The Data Protection Lead (Lynsey Crossman) is responsible for overseeing compliance with this policy and addressing data protection queries.
- Recruitment/HR Team: The Recruitment and HR team is responsible for the secure collection, storage, and management of applicant data during the hiring process.
- The Applicant: The applicant is responsible for ensuring that the personal data provided to the Organisation during the application process is accurate and up to date.

5. Main Body of Policy

5.1 Data Protection Principles

Under the UK GDPR, all personal data obtained and held by the Organisation must be processed according to core principles. The Organisation ensures that:

- Processing is fair, lawful, and transparent.
- Data is collected for specific, explicit, and legitimate purposes.
- Data collected is adequate, relevant, and limited to what is necessary.
- Data is kept accurate and up to date; inaccurate data is rectified or erased without delay.
- Data is not kept for longer than is necessary for the given purpose.
- Data is processed in a manner ensuring appropriate security, including protection against unauthorised processing, loss, destruction, or damage.
- Compliance is maintained regarding procedures for the international transfer of personal data.

5.2 Types of Data Held

The Organisation collects, stores, and uses several categories of personal data to carry out effective recruitment processes. Data is kept in recruitment files and computer systems. Specific data types collected include:

- Personal details: Names, previous names, title, address, phone numbers, email address, and date of birth.
- Next of kin: Name and contact details (where requested).
- Identification: Photographs (if included on CVs) or copies of driving licences/passports.
- Demographics and Health: Gender, marital status, disability information, or other medical information (for reasonable adjustments).
- Compliance: Right to work documentation.
- Equality Monitoring: Information on race and religion.
- Application Data: Information gathered via CVs, cover letters, and application forms.
- Professional History: Education details, employment history, qualifications, and references.
- Criminal Convictions: Data regarding criminal history (DBS).

5.3 Methods of Collection

The Organisation collects data directly from the applicant during the recruitment exercise. Data is also collected from third parties, including employment agencies, former employers (references), the Disclosure and Barring Service (DBS), and credit reference agencies (where applicable for finance roles).

5.4 Lawful Basis for Processing

The Organisation processes data only where a lawful basis exists. The table below categorises processing activities and the relevant lawful basis:

Activity Requiring Data	**Lawful Basis**
Checks regarding right to work in the UK	Legal obligation
Making reasonable adjustments for disabled applicants	Legal obligation
Making recruitment decisions (initial and subsequent)	Legitimate Interest: Ensuring the most suitable candidates are selected to support the charitable mission.
Making decisions about salary and benefits	Legitimate Interest: Maintaining market competitiveness and financial viability.
Making decisions about contractual benefits	Legitimate Interest: Effective organisational management.
Assessing training needs	Legitimate Interest: Ensuring applicants possess necessary skills for the role.
Dealing with legal claims	Legitimate Interest: Defending the charity against litigation.
Preventing fraud	Legitimate Interest: Protecting charitable assets and data.

5.5 Special Categories of Data

The Organisation processes special category data, including health, race, ethnic origin, religion, sexual orientation, and trade union membership. This occurs for equal opportunities monitoring and to determine reasonable adjustments for interviews or assessments.

The Organisation relies on Legal Obligation (for Health & Safety and Employment Law) and Explicit Consent (where volunteered for monitoring) to process this data.

5.6 Criminal Conviction Data

Due to the nature of the work undertaken by YMCA North Tyneside with children and vulnerable adults, the Organisation collects criminal conviction data via DBS checks. This data is used to determine suitability for the role.

The data is collected at the recruitment stage (or offer stage). The Organisation relies on the lawful basis of Legal Obligation (for regulated activity) and Legitimate Interest (for non-regulated roles where safeguarding remains a priority) to process this data.

5.7 Data Sharing and Third Parties

Internal access to applicant data is restricted to employees with responsibility for recruitment, HR, and the specific hiring managers relevant to the vacancy. All such employees receive training in GDPR compliance.

Data is shared with third parties for the following reasons:

- Referees: To verify employment history.
- Disclosure and Barring Service (DBS): To process criminal record checks.
- Recruitment Agencies: If the application was made via an agency.

The Organisation ensures data processing agreements are in place with third parties to secure data.

5.8 International Transfers

The Organisation generally does not share data with bodies outside of the UK/European Economic Area (EEA). If software providers host servers overseas, the Organisation ensures these transfers are covered by an "Adequacy Decision" or appropriate safeguards such as Standard Contractual Clauses (SCCs).

5.9 Retention Periods

The Organisation keeps data only for as long as necessary:

- Unsuccessful Candidates: Data is retained for 6 months after the recruitment exercise ends (to defend against potential tribunal claims).

- Talent Pool: If the applicant provides consent to keep details for future vacancies, data is retained for 9 months. This consent can be withdrawn at any time.
- Successful Candidates: Data is transferred to the employee personnel file and retained in accordance with the Employee Privacy Notice.

5.10 Automated Decision Making

No decision is made about an applicant solely based on automated decision-making (where a decision is taken using an electronic system without human involvement).

5.11 Individual Rights

Applicants possess the following rights regarding personal data:

- Right to be informed: To know how data is processed.
- Right of access: To request a copy of held data.
- Right to rectification: To correct inaccurate data.
- Right to erasure: To request deletion of data (in specific circumstances).
- Right to restrict processing: To request a pause in processing.
- Right to portability: To transfer data to another party.
- Right to object: To object to processing.

To exercise these rights, the applicant must contact the Data Protection Lead.

6. Related Policies

- Data Protection Policy
- Recruitment Policy
- Safeguarding Policy
- Employee Privacy Notice

7. Relevant UK Legislation

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Equality Act 2010

8. Monitoring and Review

The organisation is dedicated to ensuring our policies and procedures remain relevant, compliant and effective.

This policy will be reviewed annually, or more often if significant changes in legislation, regulations, risks or operations occur or if monitoring reveals a need.

The Data Protection Lead will oversee this process, and any necessary updates will be clearly documented, communicated and promptly implemented.

9. Appendix

A. Contact Details

For any concerns regarding data rights or to raise a complaint, the relevant contacts are:

Data Protection Lead

Name: Lynsey Crossman

Email: lynsey.crossman@ymcanorthtyneside.org

Information Commissioner's Office (ICO)

Telephone: 0303 123 1113

Website: www.ico.org.uk

Revisions

This section details all significant changes and updates made to this policy document.

Revision Number	Date of Revision	Description of Change
2	**Feb 2026**	**Updated DPO details, reformatted into new template.**