# Data Retention Policy

**Youth Start Limited**
Company Number: 16864238
Registered Office: 370 Osmaston Park Road, Derby, DE24 8FB

---

## Effective Date

1 January 2026

## Next Review Date

1 January 2027

---

## Introduction and Purpose

Youth Start Limited is committed to retaining personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. This Data Retention Policy establishes clear retention periods for different categories of personal data and sets out our procedures for securely deleting or anonymising data when it is no longer needed.

Retaining personal data for longer than necessary increases the risk of data breaches, creates unnecessary storage costs, and may breach data protection legislation. Conversely, deleting data too early may prevent us from fulfilling our legal obligations, defending against potential claims, or providing effective services to our clients and mentorship participants.

This policy ensures that we strike an appropriate balance between these considerations and comply with the storage limitation principle established by the UK General Data Protection Regulation (UK GDPR). It applies to all personal data processed by Youth Start, regardless of format or location.

---

## Scope

This Data Retention Policy applies to:

- All personal data held by Youth Start Limited in any format (electronic or paper-based)
- All staff members, volunteers, external mentors, and contractors who process personal data on behalf of Youth Start
- All systems and storage locations where personal data is held, including our CRM system (ZohoCRM), password-protected USB backup drives, email systems, and paper files
- All categories of individuals whose data we process, including job applicants, employers, website visitors, and mentorship participants

This policy covers retention periods, deletion procedures, and responsibilities for ensuring compliance with retention schedules.

---

## Legal and Regulatory Requirements

Our data retention practices are governed by the following legal and regulatory requirements:

**UK GDPR and Data Protection Act 2018:**
We must retain personal data only for as long as necessary for the purposes for which it was collected. We must establish and document retention periods for different categories of personal data.

**Equality Act 2010:**
We must retain recruitment data for a minimum of six months following the end of the recruitment process to defend against potential discrimination claims brought by unsuccessful applicants.

**Employment Law:**
We must retain certain employment-related data for specified periods to comply with tax, national insurance, and employment tribunal requirements. Although Youth Start does not directly employ the young people we place, we supervise employer compliance with these requirements.

**Limitation Act 1980:**
Legal claims for breach of contract or negligence can be brought up to six years after the event. We retain data necessary to defend against potential claims for a minimum of six years where appropriate.

**Financial and Tax Regulations:**
We must retain financial records, including invoices and payment records, for a minimum of six years for HMRC compliance purposes.

---

## Data Retention Schedules

We have established the following retention periods for different categories of personal data:

### Job Applicants

**Unsuccessful Applicants:**
We retain personal data from unsuccessful applicants (including application forms, CVs, interview notes, and assessment records) for a minimum of six months following the end of the recruitment process. This retention period allows us to defend against potential discrimination claims under the Equality Act 2010.

After six months, we securely delete all personal data relating to unsuccessful applicants, unless the individual has provided explicit consent to remain on our talent pool for future opportunities. Where consent has been provided, we retain data for a maximum of two years and seek fresh consent before this period expires.

**Successful Applicants:**
Personal data from successful applicants is retained for the duration of the mentorship programme plus a minimum of six months following completion of the programme. This allows us to monitor outcomes, provide ongoing support if needed, and defend against potential claims.

After this period, we anonymise outcome data for impact evaluation and research purposes. Anonymised data cannot identify individuals and is retained indefinitely to demonstrate the effectiveness of our services and contribute to evidence on youth employment outcomes.

## Mentorship Participants

**Mentorship Records:**
We retain records of mentorship calls, progress notes, support interventions, and feedback forms for the duration of the 12-week mentorship programme plus a minimum of six months following completion. This retention period allows us to evaluate the effectiveness of our mentorship approach, provide ongoing support if needed, and defend against potential claims.

After six months following completion of the mentorship programme, we anonymise this data for impact evaluation purposes. Anonymised data is retained indefinitely.

**Sensitive Personal Data:**
Where mentorship participants have disclosed sensitive personal data (such as information about health conditions, disabilities, or personal circumstances), we retain this data only for as long as necessary to provide appropriate support. We review the necessity of retaining sensitive personal data every three months during the mentorship programme and delete it promptly when it is no longer needed.

## Employer Data

**Employer Contact Details and Business Information:**
We retain employer contact details, business information, and details of recruitment requirements for the duration of our relationship with the employer plus a minimum of six years. This retention period allows us to comply with financial and tax regulations and defend against potential contractual claims.

**Employer Compliance Records:**
We retain records of employer workplace practices, compliance checks, and monitoring activities for a minimum of six years following the end of our relationship with the employer. This allows us to demonstrate that we have fulfilled our duty to supervise employer compliance with employment standards.

## Website Visitor Data

**Website Analytics Data:**
We retain website analytics data (including IP addresses, pages visited, time spent on site, and referral sources) for a maximum of 26 months. This retention period aligns with industry best practice and allows us to analyse trends in website usage over time.

**Cookie Data:**
Cookies are retained in accordance with the retention periods specified in our Cookies Policy. Most cookies expire after 12 months, although some essential cookies may have shorter expiry periods.

## Financial and Business Records

**Invoices and Payment Records:**
We retain invoices, payment records, and financial transaction data for a minimum of six years following the end of the financial year to which they relate. This retention period is required by HMRC for tax compliance purposes.

**Contracts and Agreements:**
We retain contracts with employers, data processing agreements with third-party processors, and other business agreements for the duration of the contract plus a minimum of six years following termination or expiry. This allows us to defend against potential contractual claims.

## Correspondence and Communications

**Email Communications:**
We retain email communications with job applicants, employers, and mentorship participants for the duration of our relationship plus a minimum of six months. After this period, we delete emails unless they contain information that must be retained for longer periods under other categories (for example, contractual agreements or financial records).

**Telephone Call Records:**
We do not routinely record telephone calls. Where call records are maintained (for example, logs of mentorship calls), we retain these for the same period as mentorship records (duration of programme plus six months).

## Backup Data

**USB Backup Drives:**
We retain backup copies of personal data on password-protected USB memory drives for a maximum of 30 days. Backup data is overwritten on a rolling basis to ensure that outdated data is not retained unnecessarily. Backup drives are stored in a secure location with restricted access.

**CRM System Backups:**
Our CRM provider (ZohoCRM) maintains automated backups of data stored in the system. These backups are retained in accordance with Zoho's data retention policies and are used only for disaster recovery purposes. We have documented Zoho's backup retention periods in our Data Processing Agreement.

---

## Deletion and Anonymisation Procedures

When personal data reaches the end of its retention period, we securely delete or anonymise it in accordance with the following procedures:

**Electronic Data Deletion:**
Electronic data stored in our CRM system, email systems, or other electronic storage locations is permanently deleted using secure deletion methods. Deletion is carried out by authorised personnel and is logged for accountability purposes. We ensure that deleted data cannot be recovered.

**Paper Records Destruction:**
Paper records containing personal data are securely shredded or destroyed using a cross-cut shredder. Destruction is carried out by authorised personnel and is logged for accountability purposes. We do not dispose of paper records containing personal data in general waste or recycling bins.

**USB Backup Drive Data:**
Data on USB backup drives is overwritten on a rolling 30-day basis. When a USB drive reaches the end of its useful life, it is securely destroyed to ensure that data cannot be recovered.

**Anonymisation:**
Where we wish to retain data for research, impact evaluation, or statistical purposes, we anonymise the data by removing all identifiers that could be used to identify individuals. Anonymised data includes outcome metrics, aggregated statistics, and trend analysis. We ensure that anonymised data cannot be re-identified by combining it with other data sources.

---

## Exceptions to Retention Periods

We may retain personal data for longer than the standard retention periods in the following circumstances:

**Legal Claims:**
Where we are involved in legal proceedings or anticipate potential legal claims, we retain personal data necessary to defend against those claims until the proceedings are concluded and any appeal periods have expired.

**Regulatory Investigations:**
Where we are subject to investigation by a regulatory authority (such as the Information Commissioner's Office or employment tribunal), we retain personal data relevant to the investigation until the investigation is concluded.

**Individual Requests:**
Where an individual exercises their right to restrict processing or objects to deletion of their personal data, we retain the data in accordance with UK GDPR requirements until the issue is resolved.

**Consent-Based Retention:**
Where an individual has provided explicit consent for us to retain their personal data for longer than the standard retention period (for example, to remain on our talent pool), we retain the data in accordance with the consent provided. We seek fresh consent before the consent period expires.

---

## Review and Monitoring

We regularly review our data retention practices to ensure compliance with this policy and with legal requirements. Reviews include:

**Annual Retention Schedule Review:**
We review our retention schedules annually to ensure they remain appropriate and compliant with legal requirements. We update retention periods where necessary to reflect changes in legislation, business practices, or risk assessments.

**Quarterly Data Audits:**
We conduct quarterly audits of personal data held in our systems to identify data that has reached the end of its retention period and should be deleted. Audits are documented and any issues identified are addressed promptly.

**Deletion Logs:**
We maintain logs of all personal data deletion activities, including the date of deletion, the category of data deleted, and the individual responsible for deletion. Deletion logs are retained for a minimum of three years for accountability purposes.

**Staff Training:**
All staff members who process personal data receive training on data retention requirements as part of their data protection training. Training covers retention periods, deletion procedures, and the importance of complying with retention schedules.

---

## Responsibilities

**Data Protection Lead:**
Nick Calin (contact@youthstart.co.uk, 07470435603) is responsible for overseeing compliance with this Data Retention Policy, conducting annual reviews of retention schedules, ensuring that quarterly data audits are completed, and maintaining deletion logs.

**All Staff Members:**
All staff members who process personal data are responsible for understanding and complying with retention periods, identifying data that has reached the end of its retention period, securely deleting or anonymising data in accordance with procedures, and reporting any issues or concerns to the Data Protection Lead.

**Individuals:**
Individuals have the right to request deletion of their personal data in certain circumstances under UK GDPR. Requests for deletion should be directed to contact@youthstart.co.uk. We will respond to valid requests within 30 days.

---

## Relevant Legislation

This Data Retention Policy is based on the following legislation:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Equality Act 2010
- Limitation Act 1980
- Companies Act 2006
- Income Tax (Pay As You Earn) Regulations 2003

---

## Contact Information

If you have any questions about this Data Retention Policy or wish to request deletion of your personal data, please contact us:

**Youth Start Limited**
Email: contact@youthstart.co.uk
Telephone: 07470435603
Registered Office: 370 Osmaston Park Road, Derby, DE24 8FB

We will respond to your enquiry within 10 working days.