Data Security 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 protecting the security, confidentiality, integrity, and availability of personal data and other sensitive information that we process. This Data Security Policy establishes the technical and organisational measures we have implemented to safeguard data against unauthorised access, alteration, disclosure, destruction, or loss.

Data security is a fundamental requirement of the UK General Data Protection Regulation (UK GDPR) and is essential to maintaining the trust of job applicants, employers, mentorship participants, and other individuals whose data we process. A data security breach can result in significant harm to individuals, reputational damage to Youth Start, regulatory sanctions, and financial penalties.

This policy applies to all staff members, volunteers, external mentors, and contractors who process personal data or have access to Youth Start systems and information. It establishes the security standards, procedures, and responsibilities that must be followed to protect data and systems from security threats.

Scope

This Data Security Policy applies to:

- All personal data and confidential business information processed by Youth Start Limited
- All systems, devices, and storage locations used to process or store data, including our CRM system (ZohoCRM), password-protected USB backup drives, email systems, computers, mobile devices, and paper files
- All staff members, volunteers, external mentors, contractors, and third-party service providers who process data on behalf of Youth Start
- All locations where data processing occurs, including Youth Start offices, remote working locations, and third-party facilities

This policy covers technical security measures (such as encryption, access controls, and firewalls) and organisational security measures (such as staff training, policies, and procedures).

Information Security Principles

Youth Start is committed to maintaining information security in accordance with the following principles:

Confidentiality:
We ensure that personal data and confidential information is accessible only to authorised individuals who have a legitimate need to access it. We implement access controls, authentication measures, and confidentiality agreements to prevent unauthorised disclosure.

Integrity:
We ensure that personal data and information is accurate, complete, and protected against unauthorised or accidental alteration or destruction. We implement controls to detect and prevent unauthorised changes to data.

Availability:
We ensure that personal data and systems are available to authorised users when needed. We implement backup and recovery procedures to protect against data loss and system failures.

Accountability:
We maintain records of security measures, access logs, and security incidents to demonstrate compliance with security requirements and enable investigation of security breaches.

Technical Security Measures

We have implemented the following technical security measures to protect data and systems:

Encryption

Data in Transit:
All personal data transmitted between systems, devices, or networks is encrypted using industry-standard encryption protocols. Our website uses SSL/TLS encryption to protect data transmitted between users' browsers and our web servers. Email communications containing sensitive personal data are encrypted where technically feasible.

Data at Rest:
Personal data stored in our CRM system (ZohoCRM) is encrypted at rest using industry-standard encryption. Password-protected USB backup drives use hardware or software encryption to protect data stored on the drives. We ensure that encryption keys are stored securely and are accessible only to authorised personnel.

Access Controls

User Authentication:
All users accessing Youth Start systems must authenticate using unique usernames and strong passwords. Passwords must be at least 12 characters long and include a combination of uppercase letters, lowercase letters, numbers, and special characters. Passwords must be changed every 90 days.

Multi-Factor Authentication:
Where available, we implement multi-factor authentication (MFA) for access to critical systems, including our CRM system and email accounts. MFA requires users to provide two or more forms of authentication (such as a password and a one-time code sent to a mobile device) before gaining access.

Role-Based Access:
Access to personal data and systems is granted on a need-to-know basis according to job roles and responsibilities. We implement role-based access controls to ensure that users can access only the data and systems necessary to perform their duties. Access rights are reviewed regularly and revoked promptly when no longer needed.

Access Logs:
We maintain logs of user access to systems and personal data. Access logs record the date, time, user identity, and actions performed. Logs are reviewed regularly to detect unauthorised access or suspicious activity.

Network Security

Firewalls:
We implement firewalls to protect our network from unauthorised access and malicious traffic. Firewalls are configured to block unauthorised inbound and outbound connections and are regularly updated to address emerging threats.

Antivirus and Anti-Malware:
All computers and devices used to process personal data are protected by up-to-date antivirus and anti-malware software. Software is configured to scan files and systems automatically and to update virus definitions regularly.

Secure Wi-Fi:
Where Youth Start operates Wi-Fi networks, these networks are secured using WPA2 or WPA3 encryption and strong passwords. Guest Wi-Fi networks are segregated from internal networks to prevent unauthorised access to systems and data.

Backup and Recovery

Regular Backups:
We maintain regular backups of personal data and critical systems to protect against data loss due to hardware failure, cyberattacks, or human error. Backups are stored on password-protected USB drives and are retained for a maximum of 30 days on a rolling basis.

Backup Security:
Backup drives are encrypted and stored in a secure location with restricted physical access. Backup procedures are documented and tested regularly to ensure that data can be recovered in the event of a disaster.

Disaster Recovery Plan:
We maintain a disaster recovery plan that sets out the procedures for recovering data and restoring systems following a major incident. The plan is reviewed and tested annually to ensure it remains effective.

Software and System Updates

Patch Management:
We apply security patches and updates to operating systems, applications, and software promptly to address known vulnerabilities. Critical security patches are applied within 14 days of release.

System Monitoring:
We monitor systems for security vulnerabilities, unusual activity, and performance issues. Monitoring tools generate alerts when potential security threats are detected, enabling prompt investigation and response.

Organisational Security Measures

We have implemented the following organisational security measures to protect data and systems:

Staff Training and Awareness

Data Security Training:
All staff members, volunteers, and external mentors who process personal data or have access to Youth Start systems are required to complete data security training. Training covers password security, phishing awareness, secure data handling, incident reporting, and the importance of confidentiality.

Training is provided to all new staff members before they are granted access to systems and is refreshed annually for all staff members.

Phishing Awareness:
We provide regular phishing awareness training to help staff members recognise and report phishing emails and other social engineering attacks. Staff members are encouraged to report suspicious emails to the Data Protection Lead for investigation.

Confidentiality Agreements

Staff Confidentiality:
All staff members, volunteers, and external mentors are required to sign confidentiality agreements before being granted access to personal data or confidential business information. Confidentiality agreements establish the obligation to maintain the confidentiality of data and prohibit unauthorised disclosure.

Third-Party Confidentiality:
Third-party service providers and contractors who process personal data on behalf of Youth Start are required to sign Data Processing Agreements that include confidentiality obligations. We ensure that third parties implement appropriate security measures to protect data.

Physical Security

Secure Storage:
Paper files containing personal data are stored in locked cabinets or secure storage areas with restricted access. Access to secure storage areas is limited to authorised personnel only.

USB Backup Drives:
Password-protected USB backup drives are stored in a locked cabinet or secure location when not in use. Access to backup drives is restricted to the Data Protection Lead and authorised personnel.

Clear Desk Policy:
We implement a clear desk policy requiring staff members to secure or lock away personal data and confidential documents when not in use and at the end of each working day. Computer screens must be locked when staff members leave their desks.

Visitor Access:
Visitors to Youth Start premises are required to sign in and are accompanied by a staff member at all times. Visitors do not have access to areas where personal data is processed or stored.

Secure Data Handling

Email Security:
Staff members must not send personal data or confidential information via unencrypted email unless absolutely necessary. Where sensitive personal data must be sent by email, it should be password-protected or encrypted.

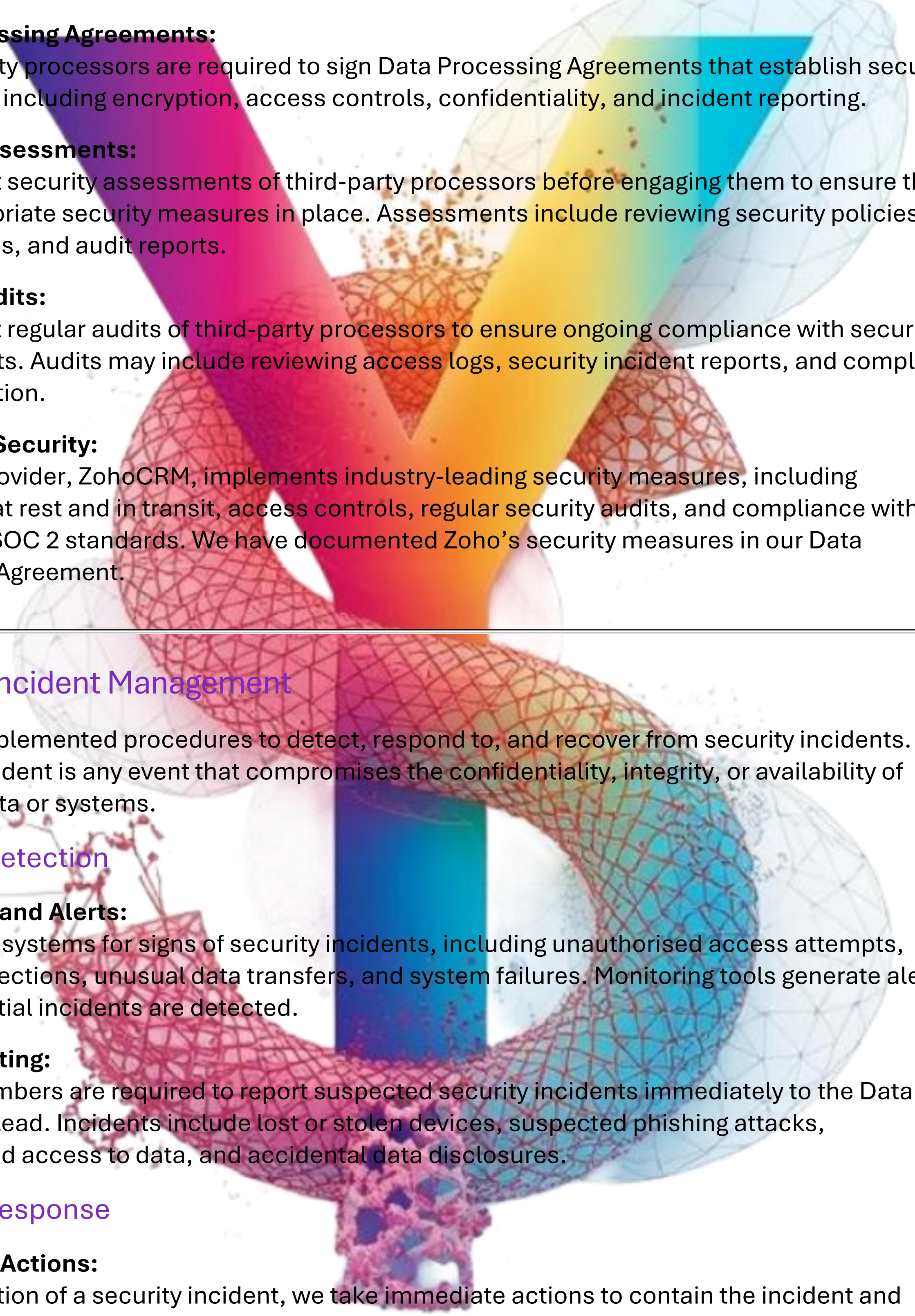
Portable Devices:
Laptops, tablets, mobile phones, and USB drives containing personal data must be password-protected and encrypted. Portable devices must not be left unattended in public places or vehicles.

Printing and Photocopying:
Staff members must collect printed or photocopied documents containing personal data immediately and must not leave documents unattended on printers or photocopiers. Documents containing personal data must be securely shredded when no longer needed.

Remote Working:
Staff members working remotely must ensure that personal data is processed securely. Remote workers must use secure Wi-Fi connections (not public Wi-Fi), lock devices when not in use, and ensure that personal data is not visible to others (for example, family members or members of the public).

Third-Party Security

We require third-party service providers and contractors who process personal data on our behalf to implement appropriate security measures to protect data. Our requirements include:



Data Processing Agreements:
All third-party processors are required to sign Data Processing Agreements that establish security obligations, including encryption, access controls, confidentiality, and incident reporting.

Security Assessments:
We conduct security assessments of third-party processors before engaging them to ensure they have appropriate security measures in place. Assessments include reviewing security policies, certifications, and audit reports.

Regular Audits:
We conduct regular audits of third-party processors to ensure ongoing compliance with security requirements. Audits may include reviewing access logs, security incident reports, and compliance documentation.

Zoho CRM Security:
Our CRM provider, ZohoCRM, implements industry-leading security measures, including encryption at rest and in transit, access controls, regular security audits, and compliance with ISO 27001 and SOC 2 standards. We have documented Zoho's security measures in our Data Processing Agreement.

Security Incident Management

We have implemented procedures to detect, respond to, and recover from security incidents. A security incident is any event that compromises the confidentiality, integrity, or availability of personal data or systems.

Incident Detection

Monitoring and Alerts:
We monitor systems for signs of security incidents, including unauthorised access attempts, malware infections, unusual data transfers, and system failures. Monitoring tools generate alerts when potential incidents are detected.

Staff Reporting:
All staff members are required to report suspected security incidents immediately to the Data Protection Lead. Incidents include lost or stolen devices, suspected phishing attacks, unauthorised access to data, and accidental data disclosures.

Incident Response

Immediate Actions:
Upon detection of a security incident, we take immediate actions to contain the incident and prevent further harm. Actions may include disabling compromised user accounts, isolating affected systems, and securing physical locations.

Investigation:
We investigate all security incidents to determine the cause, scope, and impact. Investigations include reviewing access logs, interviewing staff members, and analysing affected systems.

Notification:
Where a security incident constitutes a personal data breach that poses a risk to individual rights and freedoms, we notify affected individuals and the Information Commissioner's Office (ICO) in accordance with our Data Breach Response procedures (as set out in our GDPR Compliance Policy).

Remediation:
We implement measures to address the root cause of security incidents and prevent recurrence. Remediation may include applying security patches, updating policies and procedures, providing additional staff training, or enhancing security controls.

Incident Records

Security Incident Register:
We maintain a security incident register recording all security incidents, the response taken, and the outcome. The register is reviewed regularly to identify trends and areas for improvement.

Security Risk Assessments

We conduct regular security risk assessments to identify potential threats to data and systems and to implement measures to mitigate those risks. Risk assessments include:

Annual Security Reviews:
We conduct comprehensive security reviews annually to assess the effectiveness of our security measures and identify areas for improvement. Reviews include evaluating technical controls, organisational measures, staff compliance, and third-party security.

Threat Intelligence:
We monitor emerging security threats and vulnerabilities relevant to our systems and operations. Threat intelligence informs our security measures and helps us stay ahead of evolving risks.

Data Protection Impact Assessments:
We conduct Data Protection Impact Assessments (DPIAs) for high-risk processing activities to identify and mitigate security risks to personal data. DPIAs are documented and reviewed regularly.

Responsibilities

Data Protection Lead:
Nick Calin (contact@youthstart.co.uk, 07470435603) is responsible for overseeing data security, implementing and maintaining security measures, conducting security risk assessments, managing security incidents, ensuring staff training is provided, and ensuring compliance with this Data Security Policy.

All Staff Members:
All staff members, volunteers, and external mentors are responsible for understanding and complying with data security requirements, using strong passwords and multi-factor authentication, reporting security incidents promptly, completing data security training, maintaining confidentiality of personal data, and following secure data handling procedures.

Third-Party Processors:
Third-party service providers and contractors who process personal data on behalf of Youth Start are responsible for implementing appropriate security measures, complying with Data Processing Agreements, reporting security incidents promptly, and cooperating with security audits.

Consequences of Non-Compliance

Failure to comply with this Data Security Policy may result in disciplinary action, up to and including termination of employment or contract. Non-compliance may also result in personal liability for data breaches, regulatory sanctions, and legal action.

Relevant Legislation

This Data Security Policy is based on the following legislation and standards:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Computer Misuse Act 1990
- ISO 27001 Information Security Management Standard

Contact Information

If you have any questions about this Data Security Policy, wish to report a security incident, or have concerns about data security, please contact us immediately:

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

Security incidents should be reported immediately, even outside of normal working hours.