Data Breach Response 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 personal data of all individuals whose data we process. This Data Breach Response Policy explains how we identify, investigate, manage, and respond to data breaches in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

A data breach is a security incident that results in accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access to personal data. Data breaches can have serious consequences for individuals and organisations, including financial loss, reputational damage, and legal liability.

This policy sets out our procedures for responding to data breaches, including immediate containment measures, investigation, notification to affected individuals and regulatory authorities, and remedial actions to prevent future breaches.

This policy applies to all staff members, volunteers, contractors, and third-party processors who handle personal data on behalf of Youth Start Limited.

Scope

This Data Breach Response Policy applies to:

- All personal data processed by Youth Start Limited
- All data breaches involving personal data held by Youth Start Limited
- All systems, devices, and storage locations where personal data is held
- All staff members, volunteers, and contractors who process personal data
- All third-party processors and service providers who process personal data on behalf of Youth Start Limited

This policy does not apply to:

- Breaches involving anonymised or pseudonymised data that cannot be linked back to individuals
- Breaches that do not result in a risk to the rights and freedoms of individuals
- Breaches that are managed under separate incident response procedures (such as cybersecurity incidents that do not involve personal data)

Legal Framework

Data breach notification is required under the UK GDPR and the Data Protection Act 2018. The key requirements are:

Notification to Regulatory Authority:

We must notify the Information Commissioner's Office (ICO) of any data breach that poses a risk to the rights and freedoms of individuals, without undue delay and in any case within 72 hours of becoming aware of the breach.

Notification to Affected Individuals:

We must notify affected individuals of any data breach that poses a high risk to their rights and freedoms, without undue delay. Notification must include details of the breach, the risks involved, and the measures we have taken to address the breach.

Documentation:

We must maintain records of all data breaches, including the facts relating to the breach, its effects, and the remedial actions taken.

No Notification Required:

We do not need to notify individuals if the breach is unlikely to result in a risk to their rights and freedoms (for example, where the data is encrypted and the encryption key is not compromised).

Definition of a Data Breach

A data breach is any security incident that results in:

- Accidental or unlawful destruction of personal data
- Loss of personal data
- Alteration of personal data
- Unauthorised disclosure of personal data
- Unauthorised access to personal data

Examples of data breaches include:

- Theft or loss of a device (such as a laptop or USB drive) containing personal data
- Unauthorised access to a computer system or database
- Accidental email or document sent to the wrong recipient
- Ransomware or malware attack
- Phishing attack resulting in unauthorised access
- Breach of physical security (such as unauthorised access to an office)
- Accidental deletion or corruption of personal data
- Breach by a third-party processor or service provider

Data Breach Response Procedures

Stage 1: Detection and Reporting

Detection:

Data breaches may be detected by:

- Staff members who notice suspicious activity or missing data
- System monitoring tools that detect unauthorised access
- Third-party processors who notify us of a breach
- Affected individuals who report the breach
- External parties such as law enforcement or cybersecurity professionals

Reporting:

Any staff member who suspects a data breach must report it immediately to the Data Protection Lead (Nick Calin) using the following contact details:

Email: contact@youthstart.co.uk Telephone: 07470435603

Reports should include:

- Description of the suspected breach
- Date and time the breach was discovered
- Date and time the breach occurred (if known)
- Personal data affected
- Number of individuals affected (if known)
- Potential impact on affected individuals
- Any evidence or documentation

Confidentiality:

All reports of suspected data breaches must be treated as confidential and handled only by authorised personnel.

Stage 2: Immediate Containment

Immediate Actions:

Upon receipt of a report of a suspected data breach, the Data Protection Lead will take immediate action to:

- Contain the breach and prevent further unauthorised access or disclosure
- Isolate affected systems or devices
- Preserve evidence for investigation
- Assess the scope and severity of the breach
- Notify relevant staff members on a need-to-know basis

Containment Measures:

Containment measures may include:

- Disconnecting affected devices from the network
- Resetting passwords and access credentials
- Enabling additional security monitoring
- Blocking unauthorised user accounts
- Revoking access tokens or certificates
- Securing physical access to affected areas

Preservation of Evidence:

All evidence relating to the breach must be preserved for investigation and potential legal proceedings. This includes:

- System logs and audit trails
- Email records
- Device memory and storage
- Physical evidence (such as damaged devices or documents)

Stage 3: Investigation

Investigation Team:

The Data Protection Lead will establish an investigation team comprising:

- Data Protection Lead (investigation lead)
- IT or technical staff (if applicable)
- Relevant department heads
- External specialists (if required)

Investigation Scope:

The investigation will determine:

- What personal data was affected
- How many individuals were affected
- When the breach occurred
- How the breach occurred
- Who was responsible (internal staff, third party, external attacker)
- What systems or processes were compromised
- Whether the breach has been fully contained
- What vulnerabilities allowed the breach to occur
- What measures are needed to prevent similar breaches

Investigation Timeline:

The investigation must be completed as quickly as possible, ideally within 5 working days of the breach being reported. However, complex breaches may require additional time.

Investigation Report:

The investigation team will prepare a detailed report documenting:

- Facts of the breach
- Affected personal data
- Number of individuals affected
- Risks to affected individuals
- Root cause analysis
- Containment measures taken
- Recommendations for remedial actions

Stage 4: Risk Assessment

Risk Assessment:

The Data Protection Lead will assess the risk posed by the breach to the rights and freedoms of affected individuals. The assessment will consider:

- Type of personal data affected (sensitive data poses higher risk)
- Number of individuals affected (larger numbers pose higher risk)
- Identity of affected individuals (vulnerable individuals pose higher risk)
- Likelihood of misuse of the data
- Consequences of misuse for affected individuals
- Measures in place to mitigate the risk (such as encryption or access controls)

Risk Categories:

Breaches will be categorised as:

- **Low Risk:** Breach unlikely to result in harm to affected individuals (for example, encrypted data where encryption key is not compromised)
- **Medium Risk:** Breach may result in some harm to affected individuals (for example, unencrypted contact information)
- **High Risk:** Breach likely to result in serious harm to affected individuals (for example, unencrypted financial or health information)

Stage 5: Notification to Regulatory Authority

Notification Requirement:

We must notify the Information Commissioner's Office (ICO) of any data breach that poses a risk to the rights and freedoms of individuals, without undue delay and in any case within 72 hours of becoming aware of the breach.

Notification Details:

Notification to the ICO must include:

- Description of the breach
- Likely consequences of the breach
- Measures taken or proposed to address the breach and mitigate harm
- Name and contact details of the Data Protection Lead
- Description of the personal data affected
- Approximate number of individuals affected

Notification Method:

We will notify the ICO using the online notification form on the ICO website (https://www.ico.org.uk).

Documentation:

We will maintain records of the notification, including the date and time of notification and the response from the ICO.

Exception:

We do not need to notify the ICO if the breach is unlikely to result in a risk to the rights and freedoms of individuals. However, we must still document the breach and the reasons for not notifying the ICO.

Stage 6: Notification to Affected Individuals

Notification Requirement:

We must notify affected individuals of any data breach that poses a high risk to their rights and freedoms, without undue delay.

Notification Details:

Notification to affected individuals must include:

- Description of the breach
- Types of personal data affected
- Likely consequences of the breach
- Measures we have taken to address the breach
- Measures individuals can take to protect themselves
- Contact details for further information

Notification Method:

We will notify affected individuals using:

- Email (where email address is available and secure)
- Telephone (where telephone number is available)
- Post (where contact details are not available by other means)
- Website notification (where individual email addresses are not available)

Notification Timeline:

We will notify affected individuals without undue delay, ideally within 10 working days of the breach being reported.

Documentation:

We will maintain records of all notifications sent, including:

- Date and time of notification
- Method of notification
- Individuals notified
- Content of notification
- Responses received

Exception:

We do not need to notify affected individuals if:

- The breach is unlikely to result in a high risk to their rights and freedoms
- We have implemented appropriate technical and organisational measures to protect the data (such as encryption)
- We have taken subsequent measures to ensure the high risk is no longer likely to materialise

Stage 7: Remedial Actions

Remedial Measures:

Following a data breach, we will implement remedial measures to:

- Restore the integrity and availability of personal data
- Prevent similar breaches from occurring in the future
- Address vulnerabilities that allowed the breach to occur
- Improve security controls and processes

Examples of Remedial Measures:

- Implementing or upgrading encryption
- Implementing or upgrading access controls
- Implementing or upgrading system monitoring
- Providing additional staff training on data security
- Updating data security policies and procedures
- Conducting security audits and risk assessments
- Engaging external cybersecurity specialists
- Implementing multi-factor authentication
- Updating incident response procedures

Implementation Timeline:

Remedial measures will be implemented as quickly as possible, ideally within 30 days of the breach being reported. Complex measures may require additional time, but progress will be monitored and documented.

Monitoring:

We will monitor the effectiveness of remedial measures and make adjustments as necessary.

Responsibilities

Data Protection Lead:

Nick Calin (contact@youthstart.co.uk, 07470435603) is responsible for:

- Receiving and investigating reports of suspected data breaches
- Coordinating the data breach response
- Assessing the risk posed by the breach
- Notifying the ICO and affected individuals
- Implementing remedial measures
- Maintaining records of data breaches
- Reporting data breaches to senior management

All Staff Members:

All staff members are responsible for:

- Reporting suspected data breaches immediately to the Data Protection Lead
- Complying with data security policies and procedures
- Protecting personal data from unauthorised access or disclosure
- Assisting with investigation and containment measures
- Participating in data security training

IT and Technical Staff:

IT and technical staff are responsible for:

- Implementing technical containment measures
- Preserving evidence for investigation
- Assisting with investigation and root cause analysis
- Implementing technical remedial measures
- Monitoring systems for signs of breach

Third-Party Processors:

Third-party processors are responsible for:

- Reporting data breaches to Youth Start immediately
- Assisting with investigation and containment measures
- Implementing remedial measures
- Maintaining records of data breaches

Senior Management:

Senior management is responsible for:

- Receiving reports of data breaches
- Approving notification to the ICO and affected individuals
- Approving remedial measures
- Monitoring the effectiveness of data breach response procedures

---

Record Keeping

We maintain records of all data breaches, including:

- Date and time the breach was discovered
- Date and time the breach occurred (if known)
- Description of the breach
- Personal data affected
- Number of individuals affected

- Risk assessment and risk category
- Investigation findings
- Containment measures taken
- Notification to the ICO (date, time, and details)
- Notification to affected individuals (date, time, method, and details)
- Remedial measures implemented
- Effectiveness of remedial measures
- Lessons learned

These records are retained for 3 years after the breach is resolved.

Communication and Transparency

Internal Communication:

We will communicate information about data breaches to relevant staff members on a need-to-know basis. All communications must be confidential and handled securely.

External Communication:

We will communicate information about data breaches to affected individuals, the ICO, and other relevant parties in a clear, transparent, and timely manner.

Media and Public Communication:

We will not make public statements about data breaches without approval from senior management. Where media or public communication is necessary, we will ensure that information is accurate, transparent, and complies with legal requirements.

Training and Awareness

Staff Training:

All staff members will receive training on data security and data breach response procedures. Training will cover:

- How to identify potential data breaches
- How to report suspected data breaches
- Data security best practices
- Compliance with data security policies and procedures

Training Frequency:

Staff training will be provided:

- To all new staff members as part of induction
- Annually to all existing staff members
- Following any significant data breach or security incident

Awareness:

We will maintain awareness of data security issues and best practices through:

- Regular security updates and alerts
- Sharing of security news and information
- Discussion of data security at team meetings

Changes to This Policy

We may update this Data Breach Response Policy from time to time to reflect changes in legal requirements, security threats, or our data practices. We will notify relevant staff members of material changes and provide updated training as necessary.

Relevant Legislation

This Data Breach Response Policy is based on the following legislation:

- UK General Data Protection Regulation (UK GDPR), Article 33 (notification to supervisory authority) and Article 34 (communication to data subjects)
- Data Protection Act 2018
- Information Commissioner's Office (ICO) Guidance on Data Breach Notification

---

Contact Information

If you suspect a data breach or have questions about this policy, please contact:

Data Protection Lead: Nick CalinEmail: contact@youthstart.co.uk Telephone: 07470435603

Youth Start Limited Registered Office: 370 Osmaston Park Road, Derby, DE24 8FB

Information Commissioner's Office (for reporting breaches):

Website: https://www.ico.org.ukTelephone: 0303 123 1113

Data Breach Response Checklist

Action	Responsibility	Timeline
Report suspected breach	Any staff member	Immediately
Contain breach	Data Protection Lead / IT	Immediately
Investigate breach	Investigation team	5 working days
Assess risk	Data Protection Lead	Within investigation
Notify ICO	Data Protection Lead	Within 72 hours
Notify affected individuals	Data Protection Lead	Within 10 working days
Implement remedial measures	Relevant staff / IT	Within 30 days
Document breach	Data Protection Lead	Ongoing
Review effectiveness	Data Protection Lead	30 days after remedial measures