HR10 - GDPR, Data Breach and Data retention Policy

Reviewed: June 2025

Reviewed by Carrie Collins. Head of HR

This policy outlines how New Reflexions manages personal data to comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It ensures that personal data is retained only for as long as necessary and disposed of securely. It applies to all personal data processed by New Reflexions, including employee, young people in our care, suppliers, and external bodies information.

When personal information is collected, the 'data subject' (i.e. the person who the information is about) must be told. This is known as a Privacy Notice. This can be found on our website - https://www.newreflexions.co.uk

New Reflexions does not collect biometric data such as fingerprints or facial recognition. However, CCTV is used in some locations for security and monitoring, as outlined in the Home Statement of Purpose, School CCTV Policy, and at Head Office for external surveillance. Any enquiries about the CCTV system should be directed to enquiries@newreflexions.co.uk.

Photographs and videos

We may take photos and videos of individuals in our homes as part of our work. Written consent will be obtained from parents/carers or students aged 18+ for use in communication, marketing, and promotional materials. Staff will be consulted before using images for internal purposes like ID cards or social media.

Data Retention Principles

- Lawfulness, Fairness, and Transparency: Personal data will be processed lawfully, fairly, and transparently.
- Purpose Limitation: Data will be collected for specified, legitimate purposes and not further processed in a manner incompatible with those purposes.
- Data Minimisation: Only data necessary for the intended purposes will be collected.
- Accuracy: Personal data will be accurate and kept up to date.
- Storage Limitation: Personal data will be kept in a form which permits identification of data subjects for no longer than is necessary.
- Integrity and Confidentiality: Personal data will be processed securely.

Retention Periods

Personal data will be retained for the following periods:

- Residential Homes Management and Administration - 15 years from date created.
- Looked After Children - Until the individual's seventy fifth birthday (England and Wales) 100 years after the date of birth (Scotland)
- Accounting and Reporting - 6 years after end of financial year
- Banking Administration - 6 years after end of financial year

- Budgets Management - 6 years after end of financial year
- Payroll Administration - 6 years after end of financial year
- Pension Fund Management - 6 years after end of scheme
- Pension Scheme Administration - 6 years after death of last known beneficiary of member
- Accident and Incident Reporting and Investigation (Adults) - 3 years after investigation (non-child specific)
- Human resources main file – 7 years after termination of employment
- Human resources employee skeleton information including safeguarding – permanent
- Education – Whole record until the child's 25th Birthday

These periods are based on legal requirements and best practices. Specific retention periods may vary depending on the nature of the data and contractual obligations.

Data Destruction

Once the retention period has expired, personal data will be securely destroyed by shredding physical documents, permanently deleting electronic files, and anonymising data where appropriate

Responsibilities

- nominated Person: Oversees data protection compliance and retention schedules.
- Management Team: Ensure adherence to retention periods within their departments.
- Employees: Comply with data retention and destruction procedures.

Reporting Security Incidents

New Reflexions is committed to monitoring and responding to any incidents that may breach the security or confidentiality of its information. All incidents must be promptly identified, reported, investigated, and tracked to help prevent future occurrences.

The Nominated Person – Head of HR must be notified of any incident or breach within 24 hours of it being discovered.

All staff, including permanent, temporary, and contractors, must understand and follow the procedures for reporting incidents that could affect the security of New Reflexions' information.

What Is a Data Breach?

A data breach can include:

- Loss or theft of devices such as mobile phones, laptops, or other IT equipment.
- Personal information sent to the wrong person by email, post, or fax and accessed by an unauthorised individual (e.g., a lost file containing personal data).
- Failing to keep information secure, such as leaving documents with personal details on your desk overnight.

What Should I Do If I Suspect a Data Breach?

Outside Normal Working Hours - Report the breach as soon as possible, within 24 hours of the incident, to your line manager.

During Normal Working Hours - Inform your line manager immediately. They will notify the relevant parties (e.g. HR), and ensure the incident is recorded and investigated within 24 hours.

If the breach involves theft or a crime, your manager must report it to the police and obtain a crime reference number. If it involves IT equipment, also inform the Finance department.

Information to Provide When Reporting:

- Crime reference number (if applicable)
- Police station and constabulary (if applicable)
- Date, time, and location of the incident
- Names of employees, teams, or third parties involved
- Summary of the data lost, stolen, or shared in error
- List of individuals affected or potentially at risk
- Who else has been notified within the organisation

Line Manager Responsibilities:

- Assess the risk level of the breach
- Agree on immediate actions and assign responsibilities
- Identify who needs to be informed (internally and externally)
- Assign an investigator
- Discuss with the Head of HR to determine if the incident should be reported to the ICO (if the matter meets the threshold the Head of HR will complete the referral)
- Oversee the creation of an incident report
- Decide on remedial actions
- Share lessons learned across the organisation, if appropriate

Training

All staff are provided with data protection (GDPR) training as part of their induction process to ensure that they are aware of their responsibilities. Data protection will also form part of continuing professional development, where changes to legislation, guidance or New Reflexion's processes make it necessary.