



Data Protection and Retention Policy

Policy Created by: Kathryn Carter (Business Manager)

Last Updated: October 24 (also included in staff handbook V4 Oct24)

Review Due: October 26

1. Introduction

New Leaf Triangle collects and uses personal information about staff, volunteers, students, parents or carers and other individuals who come into contact with the organisation. This information is gathered in order to enable New Leaf Triangle to provide education support services and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the organisation complies with its statutory obligations.

New Leaf Triangle is a non-profit making organisation, that processes information only to establish and maintain the support services we offer.

2. Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulations (GDPR), and UK Law. It applies to information regardless of the way it is collected, used, recorded, stored, and destroyed, and irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing and disclosure of personal data must be aware of their duties and responsibilities and adhere to this policy.

3. Roles and Responsibilities

The data controller is New Leaf Triangle as the body who processes the data.

The data protection officer (DPO) is responsible for overseeing this policy and our compliance with the law and is the first point of contact for queries about data, or for requests for data. Our DPO is

*Business Manager
New Leaf Triangle
Goadby Road
Chadwell*



LE14 4LP

All staff are responsible for adhering to the policy in the way they collect, store and process personal data, this includes contacting the DPO if ever they:

- have questions about the policy, what it means or how to apply it
- have any concerns that the policy is not being properly followed
- if they are unsure that any data that they hold or need can be processed in a lawful way

4. Data Protection Principles

The GDPR is based on data protection principles with which New Leaf must comply. The principles say that personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant, and limited to what is necessary to fulfil the purposes for which it is processed
- accurate, and where necessary, kept up to date
- kept for no longer than is necessary for the purposes for which it is processed
- processed in a way that ensures it is appropriately secure

5. Collection of Personal Data

In order to fulfil our duties as a provider of alternative education, we have a legal basis for collecting the following data:

- personal information (such as name, address, date of birth and emergency contact details)
- characteristics (such as ethnicity, language, looked after status)
- medical and welfare information (such as doctors' information, allergies, medication, and dietary requirements)
- educational needs information (such as SEN, behaviour information or individual risk assessments)
- attendance (such as school details where the student is on roll, exclusions, and sessions they have attended)
- activity and outcomes information (such as daily records, learning outcomes and progress against outcomes)
- photographs and video recordings



We collect student information on referral forms, permission forms and other related documentation (such as EHCP or risk assessment or health reports) at the time of referral and admission. We also collect student information at points during the placement when additional information is required – for example if additional permission is needed for a particular activity.

We will ask for updated information if and when information changes such as medical needs or contact details; this will be on a form or by email. Information is collected from students with parental consent. This is especially true for the taking and sharing of photographs and videos. Consent will be recorded in a central place that staff must access, check, and adhere to as needed.

6. Storage and retention of Personal Data

It is essential that the above types of data are stored securely. This means staff must avoid:

- making unnecessary copies
- downloading to personal email accounts
- taking home, unless for legitimate business reasons and ensuring secure storage at all times
- saving multiple copies of the same document
- uploading to unsecure or public platforms
- accessing the documents in a public place – eg at an internet café or in front of friends and family

Electronic data must be deleted, and paper copies securely disposed of when it is no longer required.

7. Sharing Personal Data

We do not share student information without consent unless the law and our policies allow us to do so. We will share only information that is required and only at times it is required and only to people and organisations that require it.

We share student information on the following bases

- Officials from the relevant local authority – for the purpose of registrations, attendance, progress updates
- Officials from the student's on-roll school or other registered provider – for the purpose of registrations, attendance, and progress updates,
- Transport Providers - for the purposes of student transport



- Awarding bodies - for the purpose of student awards and qualifications

If staff are in any doubt about if and how to share any data, the DPO must be consulted in the first instance.

8. Access to Data

Under data protection legislation, parents and learners have the right to request access to the information that we hold about them. Should staff be approached with such as request, please direct them to the DPO or to contact us directly through our website

<https://www.newleaftrianglectic.co.uk>

9. Data Breaches

A data breach is any instance where personal data is accidentally or unlawfully disclosed, destroyed, lost or altered or if there is unauthorised access to personal data, either in hard copy or electronic, including through cyber-attacks. Any breach or suspected breach must be reported immediately to the DPO, who will take further action as described below:

- 1) Review the circumstances and nature of the breach and, where needed alert an NLT director to assist in ongoing investigation, containment, reporting to police and follow up actions.
- 2) Take steps to halt the breach (if still ongoing), and to minimise reach and impact of the breach, including notifying the bank of any financial risks, and pausing access to email accounts, changing any access codes or passwords as needed.
- 3) Inform the Information Commissioner's Office (ICO) within 72 hours including any known or risk of impact on individuals, communities or groups – eg if released emails may become involved in phishing attacks.
- 4) Agree a Plan of communications to individuals who may be initially affected
- 5) A full investigation will then be undertaken, with follow up communications to all involved in the steps taken to rectify and reduce further risks.

10. Further Advice

Our Data Privacy notice to parents, students, providers and the public is available on our website at <https://www.newleaftrianglectic.co.uk> and should be read in conjunction with this policy.