Data Protection Policy

NALA
National Adult Literacy Agency
Áisíneacht Náisiúnta Litearthachta do Aosaigh

Contents

Introduction

The General Data Protection Regulation (GDPR) and the Irish Data Protection Legislation tells us and other organisations how we must handle personal data.

'Personal data' means any information about people we collect. There is a list of definitions at the end of this document.

We are committed to complying with the data protection legislation.

This Data Protection Policy covers:

- how NALA handles and protects any personal data we gather to make sure that we comply with these laws
- the rights of data subjects when we handle their data
- how individuals can access any data we hold about them
- what we do if anything happens to personal data, for example if we lose it or someone else accesses it.

We gather data about:

- employees
- learners
- clients
- our members
- our suppliers
- other individuals.

These are our 'data subjects'.

This means that we control data and we are a 'data controller'.

What data is covered by this policy?

Our policy covers all the data, including personal and sensitive details that we collect about people. It covers data held on paper and on computers.

1. Our responsibilities

Data controller

NALA is considered a ‘data controller’.

A data controller is responsible for deciding how to use and protecting the data of its data subjects.

Data Protection Officer

GDPR requires some organisation to designate a Data Protection Officer ‘DPO’. NALA is not required to have a DPO due to the type and volume of data we process. However, the Chief Executive Officer ‘CEO’ has overall responsibility for ensuring compliance with the relevant data protection legislation. The CEO is supported by the Governance and Compliance Officer in overseeing compliance with the data protection requirements.

Technical and organisational systems

We have technical and organisational systems to manage data. We have designed these to make sure we can protect it. We update these systems as needed.

These systems also mean that we can clearly show that we use data appropriately.

How the systems work

Security

We have put in place high security standards to protect data, such as encryption,

password protection and two factor authentication.

Access

Only those who have the appropriate authorisation may access personal data.

Backup

If there is ever an incident affecting our systems, we can restore the availability and access to data in a timely manner.

Training

We hold frequent data protection training activities for all our employees.

Constant vigilance

We regularly test, assess and evaluate how effective our organisational and technical measures are.

Our systems are designed to protect data

(Data protection by design and default, GDPR Article 25)

When we are planning to introduce new systems or technologies, one of the first things we do is decide how to make sure we can continue to protect data. The European Data Protection Board (EDPB) encourages data controllers like NALA to plan their systems in this way.

For example, all our new network folders are accessible only to those who need access to carry out their role in the organisation.

In this way, our technical and organisational systems protect the rights and freedoms of people whose data we have.

Records of Processing Activities 'ROPA' – keeping details of how we use data

(Records of processing activities, GDPR Article 30)

We keep a record of how we use data as required by the legislation. We review this regularly and will make it available to the Data Protection Commission on request.

If there are any significant changes to an existing process or if we put in place a new process, the relevant manager must update the ROPA.

Information we have on our ROPA

Name and contact details of:

- the data controller or joint controller
- controller's representative
- relevant contact person.

We also keep a record of:

- the types of business systems we use
- categories of data we hold
- why it is legal for us to use data in the way that we do
- how long we can keep each type of data for
- when and why we share data with another organisation
- when we have transferred data to a third country, and what country that is
- the type of technical and organisational security measures we have put in place.

How we share data with other organisations

('Processor' and 'Transfers subject to appropriate safeguards', GDPR, Articles 28 and 46)

We will not share personal data with any other organisation unless there is lawful reason for us to do so or to provide a service that has been requested. Where necessary, we will ask for consent to share information with another organisation. Before we share any data with any other organisation, we put a written agreement in place. It includes how this data will be handled.

The agreement states:

A. why data needs to be shared between us and a third party
B. the right to terminate processing that we or the third party can take
C. the third party may not transfer data to any other person or organisation
D. if the third party is asked for data, they will provide it to us
E. the right for us to audit the data that the third party holds.

By 'third party' we mean anyone or organisation, whether a part of NALA or outside NALA, who manages data on our behalf.

Transfer of data outside of the European Economic Area

We will only transfer personal data outside of the European Economic Area (EEA) if we can make sure it will be protected appropriately.

In June 2021, the European Commission adopted new Standard Contractual Clauses (SCCs) to do with appropriate safety for transferring data outside the EEA. Before we undertake to transfer any data or to put new SCCs in place, we will conduct a 'Transfer impact assessment'. This will make sure that the SCCs are effective. If we find they are not effective, we will make sure that they are changed to reach the required standard.

Special Category Data

Special Category Data is:

- personal data revealing:
  - racial or ethnic origin
  - political opinions
  - religious or philosophical beliefs, or
  - trade union membership, and
- personal data concerning:
  - health or
  - a natural person's sex life or sexual orientation
- genetic data or biometric data processed for the purpose of uniquely identifying a natural person.

Where NALA processes special category data we will only do this with explicit consent unless it is necessary:

- to exercise our rights or another persons rights in relation to employment and social security or to establish the working capacity of our employees
- to protect the vital interests of an individual
- to exercise or defend a legal claim
- for reasons of substantial public interest, public health or archiving in the public interest.

If our security fails and there is a 'data breach'

A 'data breach' is a gap in security that leads to the accidental or illegal destruction, loss, alteration, unauthorised disclosure of, or access to personal data. An example of a breach is when correspondence is sent to an unauthorised third party.

We regard any loss of data in paper or digital form to be a data breach.

If there is a suspected data breach, our employees must notify the Governance and Compliance Officer. The management team along with the Governance and

Compliance Officer will assess the severity of the breach. Where necessary they will notify the Data Protection Commission within 72 hours.

Where a breach is likely to result in a high risk to the rights and freedoms of the people whose data has been compromised, we will notify those people about the breach.

Please refer to Section 4 for more information on Data Breaches.

We assess new data gathering systems

We have a system for assessing the impact of all new types of data processing. This is called a 'Data Protection Impact Assessment' (DPIA). We will share a copy of the DPIA with our Governance and Compliance Officer. They will review the DPIA and provide advice where required.

If we cannot find ways to reduce any high risks identified in a DPIA, we will consult the Data Protection Commissioner before we begin using the new system.

Record keeping

We keep logs of relevant data protection related events, for example:

- if you ask us for any of your legal rights discussed in section 'Your data and your rights' to be respected
- when data is used inappropriately
- when we carry out an assessment to see if we need to do a Data Protection Impact Assessment (DPIA).

Responsibilities of staff and others

Anyone who processes data on our behalf must comply with this data protection policy. All records created on our behalf belong to us.

Anyone who handles data we hold must read, understand and accept all our:

- data protection policies
- procedures
- guidelines.

They must also make sure that when they access, manage and control data as part of their daily duties, they do so in line with data protection requirements.

Everyone who handles data on our behalf must also make sure they comply with our data protection rules.

2. Six ways NALA protects data

There are six things we do to make sure we handle personal data appropriately.

1. We are lawful, fair and clear

We will handle personal data:

- in line with the law
- in a fair way

We will be clear about why we need the data and we will explain this.

Lawful

Generally, how we handle data is based on legislation under the Data Protection Act 2018, Section 71(1) and GDPR Article 6.1.

We can only process personal data if one or more of the following apply:

- We have been given consent to process it for one or more specific purposes. Getting consent means we will ask permission to handle personal data when necessary. Consent can be withdrawn at any time. We must process it to fulfil our duties if we have entered into a contract or to prepare for entering into the contract
- We are required by a law to process it
- It is needed to protect someone's 'vital interests'
- We must process it to carry out a task in the public interest
- We have legitimate interests that require us to process data to pursue these interests. In this case the fundamental rights and freedoms of the data subject take priority over our interests.

Fair

We will only handle data in ways that people would reasonably expect us to do so, and we will not use data in ways that might damage someone unfairly. We must do this if we got the data directly or from other sources.

Clear

We will provide necessary information about our data processing when needed. When we provide information we make sure it is:

- detailed and specific
- clear and in plain language.

We make information available through our:

- websites
- forms
- publications.

2. We gather data only as needed to provide services

We design systems to collect data so we can gather and use it:

- only for the purpose for which we collect it
- so we can provide the service asked for.

This applies to:

- online forms
- online systems
- hard copy documents
- any other ways of collecting data we might use.

Our employees must only accept a request for data from another organisation or person if it is directly related to the reason we collected the data in the first place. Even if the reason seems related, our staff must not reveal data unless it is why we originally collected the data.

If we need to give data to another organisation or person we must first assess the impact this will have before sharing it and ensure the organisation also complies with the relevant data protection legislation.

This assessment is called a 'Data Protection Impact Assessment' (DPIA).

3. Accuracy

We will make sure any data we keep about people is accurate and up to date. We need to do this so we can provide our services.

We design the ways we collect data so that it is easy to update information when we get new data.

If we have provided data to third parties which is no longer accurate, we will give them the updated data.

However, we will not do this if it is impossible or requires significant time or effort to do so. For example, if someone changes their mobile number and we do not have any other contact data to reach them.

4. We will keep your data only for as long as needed

The legislation says we should keep any personal data only for as long as we need it to provide our service.

We put in place policies and procedures to make sure that we keep personal data for the least amount of time needed so we can operate effectively.

We have systems in place to identify and destroy or remove personal data after we no longer need it.

5. Security

The law requires us to use technical and organisational security measures when handling data to protect against:

- unauthorised or unlawful access
- accidental loss, destruction or damage.

We have put in place the necessary measures to do this.

6. Accountability

We are accountable for, and able to show how we comply with the data protection legislation. We do this by using appropriate records and systems for handling personal data.

3. Individuals' rights

The Data Protection Act 2018 details what individuals' rights are when we handle their data. We design and maintain appropriate policies, procedures and staff training to make sure we fulfil the legal rights related to data protection.

'Access' personal data

(Right of access by the data subject, GDPR, Article 15)

Individuals have the right to access any of thier data which is being processed by us. We put in place ways of working that make sure when we are asked for details of data we hold, we can find and provide the data. We do this within the time allowed in the legislation.

'Rectification' – correct personal data

(Right to rectification, GDPR, Article 16)

If we hold inaccurate or incomplete data, individuals have the right to ask us to correct it.

We have systems in place to make sure that we can correct data that is inaccurate. When we correct data, we will pass that correction on to everyone who previously received the incorrect data. We will let individuals know who these people or organisations are.

However, we will not do this if it is impossible or requires significant time or effort to do so.

'Erasure' – have personal data wiped from our records

(The right to erasure is sometimes called the 'right to be forgotten', GDPR, Article 17.)

In the following circumstances, an individual has the right to ask us to delete or remove

their data.

- We no longer need the data for the purposes it was obtained.
- Consent is withdrawn and there is no legal reason why we should hold on to it.
- They object to us handling their data and there are no good reasons for us to do so.
- We are illegally processing the data.
- The law requires us to delete the data.

If this is possible we will do so.

In some cases, there may be some legal reason why we cannot remove data. For example, where we must continue to hold it:

- to exercise the right of freedom of expression, such as journalistic, academic, artistic or literary purposes
- to comply with a legal obligation
- for public health reasons
- for archiving, research, or statistical purposes in the public interest
- to set up, exercise or defend any legal claims.

If we have made any of the data public, we must take reasonable steps to contact other controllers who are processing the data. We must tell them that there has been a request for the data to be erased. However, we will only do this if we have access to the necessary technology and it is affordable for us to do so.

When we have finished dealing with a request to erase data, we will let individuals know who these people or organisations are.

‘Restriction’ – challenge how we use your data

(Right to restriction of processing, GDPR, Article 18)

We will limit how we use data if the following circumstances apply.

Inaccurate

If we are informed that personal data we hold is inaccurate, we may limit how much we

use it while we find out if this is true.

Unlawful

There is certain information for which it was unlawful for us to gather – for example, someone's ethnicity when we did not need it or we were not given consent to process it. But sometimes people volunteer this information. A person may ask us not to delete this information but instead to restrict how we use it.

Legal claims

Someone may ask us to keep their data if we no longer need it, but they need us to keep it in relation to a legal claim.

While we are answering a request

If we have been asked us to do something about the data we hold, we may be asked to limit the use of the data until we have dealt with that issue.

If we do restrict your data and we have already disclosed any of your data to others, we will tell them that the data is now restricted. However, we will not do this if it would take an undue amount of effort.

We will tell you of any other organisations or people we have told that your data is restricted.

What happens when data has been 'restricted'

If your data has been restricted, we will store it and only further use it where:

- we have consent
- it is needed for a legal claim
- we need to protect the rights of someone else
- it is needed due to important public interest like public health or safety matters.

If we later decide to use the data again, we will first write to the individual to let them know.

‘Portability’ – individuals can reuse data in more than one organisation

(Right to data portability, GDPR, Article 20)

Individuals have the right to get their data from us and reuse it across different services or in different organisations (‘data portability’). This includes data provided to us directly and any data we have gathered through dealing with people.

Where technically feasible, we must provide this data in a structured, commonly used format that a computer can understand. This allows someone to move, copy or transfer data easily from one IT environment to another. It makes this safe and secure and data easier to use.

‘Object’ –object to us using data

(Right to object, GDPR, Article 21)

An individual has the right to object to the processing of their data if it is used for:

- direct marketing
- a task carried out in the public interest
- pursuit of our legitimate interests

We may still use it if:

- we can show compelling reasons why we need to do so. These reasons must be more important than the data subject’s rights and freedoms.
- the data is needed in connection with a legal claim.
- it is being used for statistical, historical or scientific research being carried out in the public interest.

If we need to use the data in the public interest for scientific, historical or statistical research, where possible make sure that individuals cannot be identified. This is known as anonymisation.

If we have disclosed your data to others, we will tell them that you object to your data

being used. However, we will not do this if it would take undue effort.
When we have finished dealing with the objection, we will tell everyone who the decision affects. We will also tell the data subject about any other organisations or people we contacted about the request.

‘Automated decision making’ we don’t use this but if we ever do, we will ask first

(Right to opt out of automated individual decision-making, GDPR, Article 22)

Sometimes when organisations hold data, they use an automated decision system to decide things about an individual. However, if this type of decision would have a legal or significant effect on a person, they can tell the organisation not to do so.

Currently we do not use automated decision making. If we ever decide to use data in this type of system in the future, we will tell people in advance and give them the right to object.

How we go about enabling individual to access their rights

We ensure clear information is available on our website explaining:

- explaining each of the rights
- how to exercise these rights.

We will also provide this information to people in other forms such as over the phone or by post.

We put in place and maintain appropriate procedures. They enable us to assess if a requests exercise these rights can be granted.

We will write to individuals:

- confirming we received the request
- informing them if we can carry out the request
- again when we have carried out the request.

Right to complain

If an individual wishes to complain about how we use their data, they can contact our Governance and Compliance Officer.

The Governance and Compliance Officer will work with them to resolve the complaint. If they are not satisfied with how we resolved the complaint, they have a right to bring the complaint to the Data Protection Commission. The Governance and Compliance Officer will provide the appropriate contact details.

4. Data breaches

NALA is committed to its obligations under data protection legislation. We maintain a robust and structured program for compliance and monitoring. We carry out frequent risk assessments to ensure that our compliance processes and procedures are fit for purpose and that controls are in place where necessary. However, we recognise that breaches can occur so we must set out how we will deal with them if and when they do.

Categories of Data Breaches

A ‘personal data breach’ is a breach of security leading to the accidental or unlawful

- destruction
- loss
- alteration
- unauthorised disclosure • unauthorised access to personal data that is transmitted stored or being processed in any other another way.

Security breaches can be categorised as:

- **Confidentiality Breach:** where there is an unauthorised or accidental disclosure of, or access to, personal data.
- **Availability Breach:** where there is an unauthorised or accidental loss of access to, or destruction of, personal data.

- **Integrity Breach:** where there is an unauthorised or accidental alteration of personal data.

While these breaches may occur as separate incidents, depending on the circumstances, a breach may fall into more than one of the above categories.

Examples of Breaches

The following list has examples of personal data breaches where a staff member of NALA is required to start the reporting process and begin documenting the breach:

- Loss or theft of personal data, for example personal data files left in a public place
- Loss, theft or failure of equipment which stores personal data, for example theft of a laptop with personal data on it
- Unauthorised disclosure of personal data, for example an email sent to the incorrect person
- Unauthorised use of, access to, or modification of personal data or information systems, for example all staff having access to personal data files that only certain staff need for their job
- Malicious attempts to gain access to our IT systems, for example a hacker gains access to our databases
- Malicious attempts to gain access to our personal data records, for example a successful phishing attack where information is disclosed
- Loss of availability of data, for example, not being able to access our data due to a fire or flood.

Data Processor Breaches

Where NALA has engaged a third-party service provider (processor), to perform processing on the company's behalf:

- the processing activity carried out by the processor will be governed by a processing agreement in accordance with Article 28 (or Article 46 for international transfers) of the GDPR which includes a requirement for the processor to notify NALA of any breaches of data for which NALA is the data controller.

- NALA will retain overall responsibility for the protection of personal data. However, the processor is required to assist NALA in ensuring compliance with its obligations including assisting NALA in securing breached data and notifying sub-processors engaged by the processor.

Processors engaged by NALA must commit to alerting NALA without undue delay, of all potential and confirmed breaches, where NALA is the controller of the compromised personal data.

Likewise, where NALA processes data on behalf of a controller, NALA must notify the controller without undue delay of all potential and confirmed breaches.

Breach Monitoring & Reporting

NALA has appointed the Governance and Compliance Officer as the person responsible for the review and investigation of any data breach. All breaches will be investigated regardless of the severity or impact and even where a breach is fixed immediately.

Even in instances where notifications and reporting to the DPC are not required, we retain a full record of all data breaches to ensure that analysis is carried out and actions taken to prevent it happening again.

All data breaches are reported to this person and the relevant manager or CEO with immediate effect. NALA staff have detailed procedures to follow.
All data breaches are investigated.

5.Consequences of failing to comply

We take compliance with this policy very seriously. If we fail to comply, it puts individuals and the organisation at risk. Staff who fail to follow our data protection policies may be subject to disciplinary procedures.

If staff consider that this policy has not been followed, they should raise the matter

through their manager.

6. Related documents

- NALA Record Retention Policy
- NALA Subject Access Request Procedure
- NALA Data Subject Rights Procedure
- NALA Data Breach Procedure NALA Data Protection Impact Assessment Procedures
- NALA Privacy Statement

7.Definitions

Term	Definition
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Personal Data	Any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Special Category Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Data Subject	The individual to whom some personal data relates.

Data Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Officer	An appointed officer with responsibility for the Data Protection compliance of the organisation.
DPC	The Irish Data Protection Commission, (Statutory Authority)
GDPR	The General Data Protection Regulation (EU) 2016/679.
Third Party	A natural or legal person, public authority, agency or body other than the Data Subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

8. Version Control

Version	Approved by Board	Date
1.0	Yes	25 May 2018
2.0	Yes	27 April 2022
3.0	Yes	14 May 2025

The National Adult Literacy Agency (NALA) is a charity and membership based organisation. We work to support adults with unmet literacy, numeracy and digital literacy needs to take part fully in society and to have access to learning opportunities that meet their needs. NALA does this by raising awareness of the importance of literacy, doing research and sharing good practice. We also provide online learning courses and a tutoring service to adults. We lobby for further investment to improve adult literacy, numeracy and digital literacy skills.

National Adult Literacy Agency (NALA)
Sandford Lodge
Sandford Close
Ranelagh, Dublin 6
D06 YF65

Websites:
nala.ie
learnwithnala.ie

Freephone: 1 800 20 20 65

Email: info@nala.ie

Company Registration Number: 342807
Registered Charity Number: 20020965
CHY (Charity) Number: 8506