New Routes

Data Protection Policy, including key procedures

Created	**Nov 2019**
Status	**Approved**
Last Reviewed	**Feb 2022**
Author(s)	**New Routes Trustees**

Table of Contents

Aims of this Policy 3
Definitions 3
Type of information processed 4
  Clients: 4
  Volunteers: 4
  Paid staff: 4
  Trustees: 5
  Supporters: 5
  Stakeholder organisations: 5
  Delivery partners: 5
  Groups of people within the organisation who will process personal information are: 6
Responsibilities 7
Policy Implementation 8
Training 8
Gathering and checking information 8
Retention periods 9
Partnership working 12
  Other organisations we may share information on participants with: 12
Data Security 13
Procedure in case of a breach 14
Subject Access Requests 14
APPENDIX 1: Website cookies statement 15

Data Protection Policy, including key procedures

Aims of this Policy

New Routes Integration (also referred to as 'New Routes') needs to obtain and store certain information on its employees, volunteers, sessional workers, clients, trustees and partners to carry out its day-to-day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the General Data Protection Regulation 2018 and the Data Protection Act 2018. To comply with the law, personal information will be collected and used in a fair, transparent and safe manner. The legal basis for collecting and processing personal data will normally rest on New Routes' legitimate interests and consent.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

This policy covers employed staff, trustees, volunteers and sessional workers.

Definitions

In line with the GDPR 2018 data protection principles, New Routes Integration will ensure that personal data will:

- Be processed lawfully, fairly and transparently
- Be collected for specified, explicit and legitimate purposes
- Be adequate, relevant and limited to what is necessary
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures

The definition of 'Processing' is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. The organisation will seek to abide by this code in relation to all the personal data it processes, i.e.

- **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
- **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- **Consent:** The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the

purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

Type of information processed

New Routes Integration processes the following personal information:

Clients:

- Name
- DOB
- Address
- Contact details
- Country of origin
- Immigration status
- Outcomes monitoring
- Youth Consent and Emergency Contact
- Email and text message correspondence
- Meeting minutes
- Photographs

In some circumstances (notably participant registration – regarding ethnicity and health) New Routes collects data that is considered sensitive and is therefore categorised by GDPR as a 'special category'

Volunteers:

- Name
- DOB
- Address
- Contact details
- Interview form
- DBS reference number
- Signed volunteer agreements
- Mentor partnership supervision notes
- Mentor diaries
- Training attendance registers
- Volunteer meeting attendance registers
- Email correspondence
- Meeting minutes
- Photographs

Paid staff:

- Name
- DOB
- Address
- Contact details
- Recruitment data
- Contact details
- Bank and payroll details
- Supervision, appraisal and performance management information
- Staff reports
- Training and regulatory information
- Email correspondence
- Meeting minutes
- Photographs

Trustees:

- Name
- Contact details
- Address
- Training and regulatory information
- Email correspondence
- Meeting minutes
- Photographs

Supporters / event attendees:

- Name
- Contact details
- Address (where supplied)
- Email correspondence
- Photographs

Online donors:

- Name
- Contact details
- Address (where supplied)
- Email correspondence

Stakeholder organisations:

- Contact details
- Email correspondence
- Meeting minutes

Delivery partners:

- Contact details

- Partnership agreement
- Budget information
- Outcomes monitoring data
- Reports to funders
- Email correspondence
- Meeting minutes

Data collected pertaining to volunteers and participants will be stored securely electronically on our Lamplight database. Data collected pertaining to online donors will be collected and stored securely by Charities Aid Foundation (CAF) Donate, the third party we use to collect donations. The CAF Privacy Notice is available here: https://www.cafonline.org/privacy#whatpersonaldata

Original paper copies will be retained and stored securely for six years from the date of collection or until no longer relevant, whichever is later.

Groups of people within the organisation who may process personal information are:

- Employed staff
- Interns
- Trustees

Uses

We use the information given to us in order to:

- Deliver and communicate about our charitable services
- Fundraise and market our charity, events and activities
- Manage volunteers
- To check your suitability for a role as an employee or a volunteer
- To make referrals to other third party charities or support organisations, where we believe this to be in a client's best interests

Lawful Basis for the collection and processing of data

New Routes needs a lawful basis to collect and use personal data. The law allows for six legitimate ways to process people's personal data. Two of these are relevant to charities for the types of uses listed above.

Information is processed on the basis of a person's consent
Information is processed on the basis of the "legitimate Interests" of New Routes

In extreme situations, we may share personal details with the emergency services or local authorities if our employees believe it is in your 'vital interests' to do so. We may also share your personal information where we are compelled by law to do so.

New Routes is committed to safeguarding everyone we come into contact with, particularly children and vulnerable adults. If we identify that someone has been, or is at risk of, harm, we will share this

information with other relevant agencies. We may sometimes need to do this without consent from the individual, in line with relevant safeguarding legislation.

Consent

New Routes will ask for consent to send marketing and fundraising emails, and text messages.

If you register as a participant or volunteer and you share information about health conditions: HEALTH is considered 'special category data'. Here we rely on legitimate interests and condition A of GDPR Article 9(2) - explicit consent for the processing of such data for a specified purpose. Providing NR with further information on health problems is optional. Health data will be used to guarantee that New Routes can provide the best service and support to individuals and to signpost individuals to other appropriate support. On occasion health data may be shared with other appropriate agencies, for example, health services such as the NHS, the Wellbeing service, solicitors or the Red Cross Refugee Service, Norwich. Explicit verbal consent will be sought before this data is shared.

Sometimes New Routes may collect client/participant data on ethnicity for monitoring/evaluation purposes. ETHNICITY is considered 'special category data'. Here we rely on legitimate interests and condition A of GDPR Article 9(2) - explicit consent for the processing of such data for a specified purpose. Data will not be linked to other identifiable personal data (eg. names/addresses).

You can withdraw consent for these channels and activities at any time by contacting New Routes' Data Controller, Gee Cook.

Legitimate Interests

The law allows personal data to be legally collected and used if it is necessary for a legitimate business interest of the organisation - as long as its use is fair and balanced and does not unduly impact the rights of the individual concerned.

There are times when it is just not practical to ask a person for consent. In many situations, the best approach for New Routes and our supporters, clients, and volunteers is to process personal data because of our legitimate interests, rather than consent. If you want to change our use of your personal data for marketing and fundraising activities, you can do so at any time by contacting New Routes' Data Controller, Gee Cook.

Responsibilities

Overall responsibility for data protection rests with the Trustees. The named Data Protection Lead is Vince Ballester and they are responsible for overseeing:

- Reviewing data protection policy and related processes
- Identifying potential problem areas or risks
- Ensuring Data Protection training is undertaken by all staff and volunteers
- Notification to the Information Commissioner of any breaches
- Handling client access requests
- Approving unusual or controversial disclosures of personal data

The overall day-to-day management of processing information is the Data Controller: Gee Cook. The designated Data Controller will oversee:

- Ensuring all staff volunteers follow policy and procedure
- Ensure all staff are trained in policy and procedures
- Escalate any incidents to the Data Protection Lead

All employed staff, trustees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy will result in disciplinary proceedings for all employed staff, volunteers and trustees.

Policy Implementation

To meet our responsibilities staff and volunteers will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed, how it is stored and how it can be accessed and deleted before it is collected;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in adherence to our policies. [See section on partnership working]
- Queries about handling personal information will be dealt with swiftly.

Training

Training and awareness raising about the Data Protection Act 2018 and how it is followed in this organisation will take the following forms: On induction:

- All new staff/volunteers/trustees/interns handling data will be required to read the Data Protection Policy, familiarise themselves with the privacy notices attached to data collection and processing, and will be briefed on not disclosing passwords, keeping files locked and keeping location of keys private.
- General training/ awareness raising
- Statement in volunteer agreement

Gathering and checking information

Before personal information is collected, we will consider:

- Whether the information gathered is essential to the running of New Routes' projects
- Whether New Routes holding the information is in the interests of participants
- For how long it is essential to retain the information collected
- Legal basis assessment for data gathering activities

We will inform people whose information is gathered about the following:
- Why the information is being gathered
- What the information will be used for
- Who will have access to their information (including third parties)

We will inform people via a privacy notice that will be attached to all forms, displayed around the centre and available on our website.

We will take the following measures to ensure that personal information kept is accurate:
- Regular verbal check-ins
- Checking/updating information while completing monitoring forms

Personal sensitive information ('special category') will not be used apart from the exact purpose for which permission was given.

Retention periods

New Routes Integration will ensure that information is kept according to the following retention periods guidelines

Party	**Details**	**Retention period**	**Disposal**
Staff & trustees (where applicable)	Personnel files	6 years after employment ceases, (slimmed down format after 2 years)	Hard copies: shredded Electronic copies: Deleted from servers
	Application forms and interview notes (unsuccessful candidates)	1 year	Hard copies: shredded Electronic copies: Deleted from servers
	Letters of reference	6 years from the end of employment	Hard copies: shredded Electronic copies: Deleted from servers
	Redundancy details	6 years from the date of redundancy	Hard copies: shredded Electronic copies: Deleted from servers
	Parental leave	5 years from birth/adoption or 18 if	Hard copies: shredded

		child receives a disability allowance	Electronic copies: Deleted from servers
	Income tax, NI returns, income tax records and correspondence with IR	At least 5 years after the end of the financial year to which they relate	Hard copies: shredded Electronic copies: Deleted from servers
	Statutory maternity pay records and calculations	At least 3 years after the end of the financial year to which they relate	Hard copies: shredded Electronic copies: Deleted from servers
	Statutory sick pay records and calculations	At least 3 years after the end of the financial year to which they relate	Hard copies: shredded Electronic copies: Deleted from servers
	Wages and salary records	6 years	Hard copies: shredded Electronic copies: Deleted from servers
	Employee joining/new starter form	6 years after employment ceases	Hard copies: shredded Electronic copies: Deleted from servers
	Assessments under health & safety regulations	Permanently	
Volunteers	Volunteer interview form & volunteer agreement	6 years after volunteering ceases/end of associated project, whichever is later	Hard copies: shredded Electronic copies: Deleted from servers
	Contact information	6 years after volunteering ceases/end of associated project, whichever is later	Hard copies: shredded Electronic copies: Deleted from servers
	Attendance and work records	Data relating to programmes will be retained for as long as is necessary to provide an audit trail for funders, as set out in contractual agreements. Usually 6 years after end of project/ end of	Hard copies: shredded Electronic copies: Deleted from servers

		service access, whichever is later	
	Photographs	Indefinitely, unless consent is withdrawn	Hard copies: shredded Electronic copies: Deleted from servers
Participants/clients	Registration details	Data relating to programmes will be retained for as long as is necessary to provide an audit trail for funders, as set out in contractual agreements. Usually 6 years after end of project/ end of service access, whichever is later	Hard copies: shredded Electronic copies: Deleted from servers
	Attendance and work records	Data relating to programmes will be retained for as long as is necessary to provide an audit trail for funders, as set out in contractual agreements. Usually 6 years after end of project/ end of service access, whichever is later	Hard copies: shredded Electronic copies: Deleted from servers
	Photographs	Indefinitely, unless consent is withdrawn	Hard copies: shredded Electronic copies: Deleted from servers
General	Accident books, accident records/reports	3 years	Hard copies: shredded Electronic copies: Deleted from servers
Supporters/ Online Donors/ Event attendees	Attendance and work records	Data relating to programmes will be retained for as long as is necessary to provide an audit trail for funders, as set out in contractual agreements. Usually 6 years after end of project/ end of	Hard copies: shredded Electronic copies: Deleted from servers

		service access, whichever is later	
	Photographs	Indefinitely, unless consent is withdrawn	Hard copies: shredded Electronic copies: Deleted from servers
	Donation data	6 years after the date of our last interaction. In most cases, this represents 6 years after the last financial transaction. There are a few exceptions to this rule. If a supporter has kindly left New Routes a gift in their will we will maintain our records of that pledge indefinitely to carry out legacy administration and communicate effectively with the families of people leaving us a legacy. We also have a legal obligation to retain some financial information for seven years to allow HMRC to audit Giftaid.	Hard copies: shredded Electronic copies: Deleted from servers

Partnership working

New Routes delivers projects in partnership with a number of organisations. Partnership agreements contain reference to information sharing protocols and requirements.

The following areas of New Routes' work are covered by Information Sharing Agreements and any personnel involved in delivery of those projects will be made aware of the contents of the agreement.

- Norwich Integration Partnership – New Routes; English+; The Bridge Plus+

New Routes will ensure that all partners we work with have GDPR compliant privacy notices and will request that all new partners are aware of our Information Sharing Agreement.

Other organisations we may share information on participants with:

- English+

- The Bridge Plus+
- NCAN referral system
- NHS
- Bicycle Links CIC (Welcome Wheels Project)
- Norwich International Youth Project
- Norwich City Council
- Schools
- People From Abroad County Council team
- Job Centre
- Norfolk County Council
- Red Cross refugee service
- Age UK
- Terrence Higgins Trust

Lamplight database

New Routes is satisfied that our database providers, Lamplight, are GDPR compliant and that any data stored on Lamplight servers is only accessible to Lamplight staff members when a service is requested by New Routes, and that all Lamplight staff are bound by confidentiality agreements.

Any information shared with these organisations will always be in the best interests of the participant.

Data Security

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

- Induction on data security for all staff/volunteers working with data
- Security locks on external front door
- Using lockable cupboards and filing cabinets. Access to keys restricted to staff, sessional staff and trustees
- Password protection on all work computers, email accounts
- Password access to Lamplight database. Access to database restricted to staff members and sessional staff members with official New Routes email addresses
- Personal data can only be taken off site on password protected laptop
- All work mobile phones containing personal phone numbers will be password protected
- Data on computers will be backed up on to Microsoft One Drive. Data on our Lamplight database is held in the Lamplight cloud server.
- Online donor data is collected and stored securely by Charities Aid Foundation (CAF) Donate, the third party we use to collect donations. The CAF Privacy Notice is available here: https://www.cafonline.org/privacy#whatpersonaldata
- Some basic data relating to the City of Sanctuary project (names and email addresses) may be held securely on a password protected Google Drive account.

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary proceedings

The Board and trustees are accountable for compliance of this policy. A trustee could be personally liable for any penalty arising from a breach that they have made.

Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.

Procedure in case of a breach

When a breach of data protection occurs, consideration will be given to reviewing practices. In addition New Routes Integration will consider whether the breach should be reported to the Information Commissioner and/or to any partners with which we hold Information Sharing or Partnership Agreements.

Subject Access Requests

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Data Protection Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the DPA to access certain personal data being kept about them on computer and in certain files. Any person wishing to exercise this right should apply in writing to the New Routes Data Controller, Gee Cook, at geecook@newroutes.org.uk. The application will be approved by the Data Protection Lead.
.

The following information will be required before access is granted:

- Full name and contact details of the individual making the request
- Relationship to the organisation (former/ current member of staff, trustee, volunteer, participant, partnership colleague)
- Timescale the individual wishes to access

We may also require proof of identity before access is granted. One of the following forms of ID will be required: Passport, driving license, birth certificate, UK Gov. issued travel document, Home Office identity card

We will endeavour to deal with queries about handling personal information swiftly.
We will aim to comply with requests for access to personal information as soon as possible but will ensure it is provided within the 40 days required by the Act from receiving the written request.

This policy was adopted at the Board Meeting at New Routes Integration

APPENDIX 1: Website cookies statement

Website Cookies statement

- Our website uses cookies to improve loading speed on return visits, to properly load assets like fonts, icons and javascript, and to ensure user requests are routed to the correct server.
- It does not use cookies for analytical purposes or to track visitors' personal data.
- The cookies this website uses are provided by our hosting company (BIGipServerTethys) and by Google (_ga) whose webfont service provides our fonts.
- You can use your browser settings to disable cookies.
- Different browsers offer different levels of control – for example you may be able to accept certain cookies and reject others, such as third-party cookies.
- If you refuse cookies please be aware our websites may not work smoothly for you and there will be certain parts that won't function correctly.
- You can delete the cookies stored on your computer at any time.

Accept cookies Do not accept cookies