POLICY CONTROL PAGE

Policy Name:	Data Protection Policy
Policy Reference:	reCORP 03
Applies to:	reSource CiC and partners
Policy Version:	01
Policy Date:	January 2021
Approved Date:	January 2021
Approved By:	 Janine Cusworth Jozsef Vass
Change History	reviewed 12/1/22 no change

Alternative Format
This document is available in a variety of accessible formats including large print, Braille and electronic formats.

If you would like a copy in an accessible format, in a language other than English or would like someone to explain it to you please contact:

Janine Cusworth
Tel: 07941 914323

Email: circularresource@gmail.com

Contents

2 Policy

2.1 reSource must comply with the Data Protection Act 1998 and General Data Protection Regulations 2018 (GDPR). Please refer to section 3.

2.2 ReSource needs to use and gather certain information about individuals.

2.3 These can include

- Service Users
- Current, previous and prospective employees
- Trustees
- Volunteers
- Suppliers
- Business contacts

- Users of our websites
- Other people the organisation has a relationship with or may need to contact

2.4 Some of this data will be ‘personal data’ or ‘sensitive personal data’ as defined in section 24.

2.5 When referring to service users within this policy, we mean children, young people and adults.

2.6 This policy describes how such data must be collected, handled and stored and ensures ReSource:

- Complies with data protection law, GDPR and follows good practice
- Protects the rights of service users, employees and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach
- Considers privacy in the design of new systems and processes

2.6 Failure to comply with this policy may result in disciplinary investigation. Serious breaches could result in disciplinary action up to and including dismissal.

2.8 This policy applies to all systems, people and processes that constitute the organisation’s information systems, including Trustees, Directors, employees, suppliers, agency workers and other third parties who have access to ReSource systems.

3 Data Protection Law

3.1 The Data Protection Act (DPA) 1998 describes how organisations must collect, handle and store personal information.

3.2. The General Data Protection Regulations 2018 (GDPR) is designed to protect the personal data of citizens of the European Union.

3.3 These rules apply whether data is stored electronically, on paper or other materials but must be in a formal system.

3.4 ReSource maintains a registration notification with the Information Commissioner’s Office (ICO), which broadly outlines our data processing activities. This is publically accessible from the Register of Data Controllers' link on the ICO website.

3.5 The DPA and GDPR sets out 7 principles which ReSource will adhere to. They state -:

1. Personal data must be processed fairly and lawfully and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency)
2. Personal data must be collected for specified, explicit and lawful purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation)
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purpose (data minimisation)
4. Personal data must accurate (and up to date) (Accuracy)
5. Personal data must not be kept for longer than necessary (storage limitation). Please also refer to the Record Management Policy
6. Personal data must be kept secure (and protected from unauthorised processing, loss or destruction) using appropriate technical and organisational measures (integrity and confidentiality/security). please also refer to the IT Security policy
7. Real Life Options must take responsibility for what we do with personal data and how we comply with the other principles. We must have appropriate measures and records in place to be able to demonstrate our compliance (Accountability)

3.6 When acting as a Controller, ReSource will be responsible for, and demonstrate, compliance with the principles.

4 Rights of the Individual

4.1 The data subject has rights. These consist of:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

4.3 Each of these rights are supported by appropriate procedures within ReSource that allow the required action to be taken within the timescales stated in the DPA and GDPR. Please refer to section 10

5 Risks

5.1 This policy helps to protect ReSource and its data subjects from data security risks, including:

- Breaches of confidentiality, for example, information given out inappropriately
- Failing to offer choice, for example, all individuals should be free to choose how the organisation uses data relating to them
- Reputational damage, for example, the organisation could suffer if hackers successfully gained access to sensitive data
- Financial loss or fines – GDPR states that serious breaches of data protection regulations can result in significant fines. This could pose a significant financial risk to the organisation

6 Responsibilities

6.1 Everyone working for, or with, ReSource has some responsibility for ensuring data is collected, stored and handled appropriately The table below details role responsibilities.

Role	Responsibilities
All Staff and Volunteers	➢ Complying with the Data Protection Policies and Procedures ➢ Ensuring personal data is not disclosed to unauthorised people, either within ReSource or externally ➢ Complying with the ICT Security Policy ➢ Ensuring data is regularly reviewed. If no longer required, it should be disposed of or deleted ➢ Advising their Line Manager of any changes to processing personal data ➢ Advising their Line Manager of any changes to their own personal data requirements that their service/function is required to maintain ➢ Complying with any requests from the organisation to provide or update personal details within the requested timescales

	➢ Advising their Line Manager of a potential data breach Requesting help from their Line Manager or other appropriate person within the organisation if they are unsure of any aspect of data protection
Trustees and Directors	➢ Responsible for ensuring that ReSource meets its legal obligations that handling and storage of personal data meet acceptable security standards
Data Protection Lead	➢ Report to the highest level of authority and will be allowed to act independently in carrying out this role ➢ Keeping the Leadership Team and Directors updated about data protection responsibilities, risks and issues ➢ Ensuring all data protection policies and procedures are reviewed in line with policy review schedules ➢ Arranging payment of annual registration fees ➢ Ensuring data protection training and advice for people with responsibilities as outlined within this policy ➢ Ensuring prompt handling of requests from individuals to see the data ReSource holds about them ➢ Checking and approving any clauses in contracts or agreements with third parties that may handle the company's sensitive data ➢ Ensuring data protection investigations are carried out in line with procedures ➢ Supporting and providing advice on Privacy Impact Assessments ➢ Liaising with the ICO during any data breach report ➢ Maintaining an Information Asset Register

Managers	➢ Ensuring their staff team have read and understood the Data Protection, ICT, Record Management and Confidentiality policies ➢ Ensuring Data Protection compliance in all work activities undertaken by staff under their control ➢ Notifying the Data Protection Officer of any changes to the processing of personal data or any new information assets

7 Lawfulness of Processing

7.1 The DPA and GDPR are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

7.2 For personal data to be processed lawfully, they must be processed on the basis of one of the legal grounds set out in the DPA. There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the DPA and GDPR.

7.3 It is ReSource's policy to identify the appropriate basis for processing, and to document it in accordance with the Regulations and process in accordance with those requirements. The options are:

1. Consent	Unless it is necessary for a reason allowable in the DPA or GDPR, ReSource will always obtain explicit consent from a data subject to collect and process their data using a positive indication method. In the case of children below the age of 16 (a lower age may be allowable in specific EU member states), parental consent will be obtained. Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained, and their rights with regard to their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.

	If the personal data are not obtained directly from the data subject, this information will be provided to the data subject within a reasonable period after the data are obtained and definitely within one month. Consent will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained. Where consent is required, the relevant consent form must be completed.
2.Performance of a Contract	Where the personal data collected and processed is required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question, for example, a care at home service cannot be provided without an address to attend.
3. Legal Obligation	If the personal data is required to be collected and processed in order to comply with the law, explicit consent is not required. This may be the case for some data, for example, related to employment and taxation.
4. Vital Interests of the Data Subject	In a case where the personal data are required to protect the vital interests of the data subject or of another person, then this may be used as the lawful basis of the processing. ReSource will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data.
5. Task Carried Out in the Public Interest	Where ReSource needs to perform a task that it believes is in the public interest or as part of an official duty, the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required
6. Legitimate Interests	If the processing of specific personal data is in the legitimate interests of ReSource and is judged not to affect the rights and freedoms of the data subject in a

	significant way, this may be defined as the lawful reason for the processing and the reasoning will be documented.

8 Accountability

8.1 ReSource will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

8.2 ReSource will provide comprehensive, clear and transparent privacy notices.

8.3 Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or in relation to criminal convictions and offences.

8.4 Internal records of processing activities will be recorded.

9 Data Breach

9.1 It is Real Life Option Group's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the DPA and GDPR.

9.2 All potential breaches will be assessed and recorded in line with the data breach procedure.

9.3 Where a breach is known to have occurred and is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours.

9.4 Data breaches are discussed at the data protection sub group and lessons learnt shared as part of the data protection briefings.

10 Individual Rights

The right to be informed	If we collect personal data directly from data subjects, we will inform them via a privacy notice written in clear, plain language which is concise, transparent, easily accessible and free of charge. We will also inform data subjects, whose personal data we process, that we are the Data Controller with regard to that data, and how to contact the Data ProtectionLeadr
The Right of Access	Anyone who has personal data held by ReSource is entitled to: ➢ Ask what information the company holds on them and why ➢ Ask how to gain access to it ➢ Be informed how to keep it up to date ➢ Be informed how the company is meeting its Data Protection obligations If an individual contacts the company requesting information we hold about them, this is called a “Data Subject Access Request”. Any requests should be made to a line Manager, or via email address circullarresource@gmail.com Requests will be responded to within 30 calendar days. The person receiving the request must complete the Data Subject Access Request form and submit this to the Data Protection Lead If requests are complex or numerous, this period may be extended by a further two months. The requester must be informed of the reason for the extension within 30 days of receipt of the original request. Information given in response to a Data Subject Access Request will be all that is contained in the personal data at the time the request was made. However, it should be acknowledged that routine amendments and deletions of the data may continue between the time of the request and the date of the reply. ReSource has the right to refuse a request if:

	➢ An identical or similar request has already been made ➢ The request is unfounded ➢ The request is excessive in nature unless a reasonable interval has elapsed In deciding whether a request can be processed, the nature of the data, purpose of processing and frequency with which the data is altered will be considered. In all cases, an individual will be informed whether or not their request is to be granted. If granted, the information will be provided promptly and within no longer than 30 calendar days of the date of the receipt of the request. If a decision is made not to take action on the request, the person will be given an explanation for the decision and informed of their right to complain to the supervisory authority and seek a judicial review within 30 days of receipt of the request. Information will be generally provided free of charge unless: ➢ It is deemed unfounded or repetitive ➢ A request is made for further copies of the same information to be sent If a fee is charged, it will be based on the administrative cost of providing the information which will vary dependant on the nature of the request. When requests are made for large amounts of personal data, the DPA and GDPR Regulations permit the person receiving the request to ask the individual to specify the information the request relates to. In the event of a disagreement between a data subject and ReSource regarding personal data, the matter should be taken up under the Grievance or Complaints Policies. If complaints are not resolved through these means, you have the right to refer the matter to the Information Commissioner (www.ico.org.uk).
The right to Rectification	Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, ReSource will inform them of the rectification where

	possible. Where appropriate, ReSource will inform the individual about the third parties that the data has been disclosed to. Requests for rectification will be responded to within one month. This will be extended by two months where the request for rectification is complex. Where no action is being taken in response to a request for rectification, ReSource will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy
The Right to Erasure	Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals have the right to erasure in the following circumstances: ➢ Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed ➢ When the individual withdraws their consent ➢ When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing ➢ The personal data was unlawfully processed ➢ The personal data is required to be erased in order to comply with a legal obligation ReSource has the right to refuse a request for erasure where the personal data is being processed for the following reasons: ➢ To exercise the right of freedom of expression and information ➢ To comply with a legal obligation for the performance of a public interest task or exercise of official authority ➢ For public health purposes in the public interest ➢ For archiving purposes in the public interest, scientific research, historical research or statistical purposes

	➢ The exercise or defence of legal claims Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. In the unlikely event that personal data has been made public within an online environment, ReSource will inform other organisations who process the personal data to erase links to and copies of the personal data in question. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.
The Right to Data Portability	Individuals have the right to obtain and reuse their personal data for their own purposes. Personal data in electronic formats can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability. The right to data portability only applies in the following cases: ➢ To personal data that an individual has provided to a controller ➢ Where the processing is based on the individual's consent or for the performance of a contract ➢ When processing is carried out by automated means Personal data will be provided in a structured, commonly used and machine-readable form. ReSource will provide the information free of charge. Where technically feasible, data will be transmitted directly to another organisation at the request of the individual.

	ReSource is not required to adopt or maintain processing systems which are technically compatible with other organisations. In the event that the personal data concerns more than one individual, we will consider whether providing the information would prejudice the rights of any other individual. ReSource will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request. Where no action is being taken in response to a request for rectification, ReSource will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

11 Data Use, Storage and Security

11.1 Data use, storage and security arrangements are detailed in the ICT and Record Management procedures, but all records will not be kept longer than legally necessary for the type of record.

12 Disclosing Data for other Reasons

12.1 In certain circumstances, the DPA and GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

12.2 Under these circumstances, ReSource will disclose the requested data. However, the Data Protection Lead will ensure the request is legitimate, seeking assistance from the Leadership Team and/or the company's legal advisers, where applicable.

12.4 We may also disclose personal data we hold to third parties:

- In the event that we sell, buy or merge any business or assets. In this case, we may disclose personal data we hold to the prospective seller or buyer of such business or assets

- If we are under a duty to disclose or share a data subject's personal data in order to comply with any legal obligation, or in order to enforce or apply any contract with the data subject or other agreements; or to protect our rights, property, or safety of our employees, customers, or others. This includes exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction.

13 Contracts Involving the Processing of Personal Data

13.1 ReSource will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the DPA and GDPR.

14 Privacy by Design

14.1 ReSource has adopted the principle of privacy by design by default and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more Data Protection Impact Assessments.

15 Freedom of Information

15.1 The Freedom of Information Act 2000 (FOIA) gives a right to public access to information held by, or on behalf of, Government and other public bodies. The FOIA does not apply to companies such as those within ReSource directly. However, information provided to a public authority by ReSource may fall within the scope of the FOIA.

15.2 ReSource will comply with its responsibilities and the relevant legislation when working with public authorities or other organisations who fall within the scope of the FOIA.

16 Transferring Personal Data to a Country outside the European Economic Area (EEA)

16.1 Transfers of personal data outside the European Union will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the DPA and GDPR. This depends partly on the European Commission's judgement as to

the adequacy of the safeguards for personal data applicable in the receiving country, and this may change over time.

16.2 If we transfer any personal data we hold to a country outside the EEA, we will only do so provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms
- The data subject has given consent
- The transfer is necessary for one of the reasons set out in the DPA, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject
- Transfer is legally required on important public interest grounds or for the establishment, exercise or defence of legal claims
- The transfer is authorised by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights

16.3 Subject to the requirements in this clause above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

17 Training

17.1 All employees and volunteers receive data protection training as per of their induction and refresher training on an annual basis.

18 Further Information

18.1 Further information is available at www.informationcommissioner.gov.uk

The Information Commissioner's office is at:

Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Switchboard*:* 01625 545 700
Email: mail@ico.gsi.gov.uk
Data Protection Help Line: 01625 545 745
Notification Line: 01625 545 740