01. Confidentiality & Data Protection

1. Purpose of Policy

i. Most people will have heard of Data Protection and there has been a Data Protection Act (DPA) since 1998. This Act put a range of obligations on organisations that held data or information and also gave people the right to see any information held, although usually for a small fee. Carers Link has been registered under this Act.

ii. In May 2018, the Data Protection Act was replaced by new EU General Data Protection Regulations (GDPR). This puts stricter controls on organisations, requires greater transparency and gives individuals more rights (this time without cost). As before, GDPR applies to both computer and paper (manual) files.

iii. This purpose of this policy is to provide:
- An overview of confidentiality and how we treat confidential information (Section A)
- An overview of our GDPR compliance and how we will handle individual rights (Section B)
- An overview of how we will handle Data Breaches (section C)
- Details of additional legislation affecting personal information and/or special categories (Section D)

iv. The policy should be read as part of our suite of data/information policies, namely:
- I 01 Confidentiality & Data Protection
- I 02 Employee & Volunteer Data Policy
- I 03 ITC Policy
- I 04 Wheesht - Privacy Policy for Young Carers
- I 05 Privacy Policy for Carers

2. Definitions & Scope

i. For the purposes of brevity, the term 'staff' or 'staff member' shall include reference to any Social Work students on work placements.

ii. **Personal data** means:
- Any information which relate to a living individual who can be identified (directly or indirectly) as a result of that information or in combination with other identifiers that can be reasonably accessed.
- Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

iii. **Sensitive data** are special categories of personal data and relate to:
- A person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, sexual life, sexual orientation, genetic and biometric data and a person's physical or mental health or condition. It also includes personal data relating to criminal offences and convictions.

iv. By **processing,** we mean the act of obtaining, recording or holding the information as well as organising, amending, using, sharing, erasing and ultimately destroying the data. Processing also includes transmitting or transferring personal data to third parties.

3. Accountability & Responsibilities

i. All employees, students and volunteers having access to information regarding the company, other employees, volunteers, carers or suppliers or any other personal or confidential information will be subject to this policy and are considered under the provision of the General Data Protection Regulations.

ii. **Data Processors** are those responsible for processing personal data. As such all the staff and most volunteers are considered to be data processors (although *all* volunteers should comply with confidentiality principles). It is important to note that if you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities (this is done automatically via our new database CharityLog). You may also have legal liability if you are responsible for a breach.

iii. A **Data Controller** is the person who determines the purposes and means of processing personal data. They are also responsible for ensuring the organisation policies and processes are GDPR compliant. Within Carers Link, the Data Controllers are:
- Jennifer Roe, CEO
- Clair Hegarty, Office Manager

A. Confidentiality & Codes of Conduct

4. Personal Information Promise

i. Carers Link promises that we will:

- Value the personal information entrusted to us and make sure we respect that trust;
- Endeavour to go further than just the letter of the law when it comes to handling personal information, and adopt good practice standards;
- Consider and address the privacy risks first when we are planning to use or hold personal information in new ways, such as when introducing new systems;
- Be open with individuals about how we use their information and who we give it to;
- Make it easy for individuals to access and correct their personal information;
- Keep personal information to the minimum necessary and delete it when we no longer need it;
- Have effective safeguards in place to make sure personal information is kept securely and does not fall into the wrong hands;
- Provide training to Staff, Students and Volunteers who handle personal information and treat it as a disciplinary matter if they misuse or don't look after personal information properly;
- Put appropriate financial and human resources into looking after personal information to make sure we can live up to our promises; and
- Regularly check that we are living up to our promises and report on how we are doing.

ii. In addition, Carers Link subscribes to the 6 enforceable principles of good practice in data protection as outlined in the EU General Data Protection Regulations, namely that data or information must be:

- Fairly and lawfully processed and in a transparent manner
- Collected and processed for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Not kept longer than necessary in a form that permits identification
- Secure including protection against unauthorised use or accidental loss, destruction or damage.
- Not transferred to countries without adequate protection

5. General Principles

i. All matters pertaining to individual carers or the people that they care for - whether derived from professional activity or from volunteer or social contact - remain confidential.

ii. All persons connected with Carers Link must hold as confidential the details of their contacts and knowledge of particular carers. Nevertheless, such information is ultimately confidential to the organisation, not the individual staff member or volunteer. This allows sharing of concerns or support needs amongst the staff (or named volunteer) involved.

iii. All persons associated with Carers Link should bear in mind that they are ambassadors for the organisation in all situations. Thus, discussion with regard to the confidential details of individual or group cases should not be entered into in a public environment such as corridors and public spaces within the offices, within local authority or other functional buildings or in any circumstance likely to be overheard by a third party.

iv. Carers Link's confidentiality and data policies observes the respect due to individuals and would ask that all individuals treat information with regard to carers, or the people that they care for, in the same way as they themselves would wish to be treated.

v. Material held on file or on computer within Carers Link must not be disclosed to any person outside the immediate professional sphere of the organisation (i.e. to any third party) and must be returned to the office as soon as possible if removed for the purpose of home visit etc.

6. Use of Information - General

i. Carers Link maintains personal data for a range of purposes. These are detailed within the additional data policies listed in the introduction (purpose) of this policy.

ii. Staff members are entitled to access some necessary personal data on Volunteers and Carers in order to provide a service.

iii. A limited number of Volunteers, selected and provided with further training, have access to some necessary personal data of Carers in order to provide ongoing support (via Carers Call) and within some service delivery areas.

iv. The Management Team will ensure that all staff and student placements receive induction on the aforementioned suite of policies.

v. The Volunteer Services Co-ordinator will ensure that all volunteers receive training on confidentiality and data protection. They will also ensure that Carers Call volunteers receive additional process training in relation to the database.

vi. All staff, students and volunteers will:

- Record only information about an individual that is necessary in order to provide them with a good quality service
- Ensure the accuracy of information before recording it and amend inaccurate records as soon as possible
- Share information (see section 4 below) about individuals with colleagues only where this is necessary in order to provide them with a good quality service (e.g. discussing a case with a line manager)
- Access only such information as they need in order to carry out their agreed role within the organisation

7. Sharing of Information - General

i. Exchange of information with regard to Carers, or the people that they care for, is an acceptable practice **only** within the professional context of the work of Carers Link. This includes discussion of issues with strategic or policy implications at Board and senior Staff level; discussion of individuals with regard to care or support arrangements at Staff or Volunteer level; discussion of particular circumstances with regard to Social and Support activities at Volunteer, Staff or associated group level.

ii. However, the above policy or any confidentiality clauses within other policies will be negated if there are significant or immediate concerns about a risk of harm or injury either to the Carer by themselves or by the person they care for, or risk of harm or abuse to the person being cared for.

iii. Any concerns will be dealt with according to the appropriate policy but may involve the sharing of information to an external agency i.e. statutory, health or police.

iv. The actual or suspected abuse of a vulnerable adult or child provides sufficient grounds to warrant sharing information on a 'need to know' basis and you should avoid any unnecessary delay in passing on concerns to Social Work, the Police or other appropriate statutory body.

v. Wherever possible the consent of the vulnerable adult should be obtained prior to information being shared on his/her behalf. Where the adult is judged to not to have the mental capacity to make an informed decision - or you are aware of intimidation or coercion from others is influencing a refusal of consent - it may be necessary for you to take a professional decision to made to override the adult's expressed wishes if it is believed that the adult continues to be at risk of significant harm. Even where the adult is judged to be taking an informed and autonomous position you should consider the risks and the adult's other areas of vulnerability prior to deciding to take no further action.

vi. No consent is required when sharing information regarding actual or suspected abuse of a child or any other such concerns.

vii. Remember that Breaching Confidential / Data Protection Policies **is allowed**:

- **If sharing is to protect the vital interests of the person or another individual or**
- If sharing is for crime and taxation purposes i.e. for the prevention or detection of an unlawful act

8. Retention, Archiving & Disposal of Information

i. The aforementioned Data Policies all provide details of retention periods of the personal data of staff, volunteers and carers.

ii. Any paper/manual information that requires to be destroyed will be done so in a secure manner i.e. by professional shredding company and Carers Link will keep information which is awaiting destruction in a locked cabinet.

B. GDPR Compliance & Individual Rights

9. Compliance

i. We have reviewed the purposes of our processing activities, and selected the most appropriate lawful basis (or bases) for each activity. These are listed within the data tables appended to the policies for each organisational group (Carers, Volunteers and Staff).

ii. We have also included a statement as to the purpose for processing the personal or sensitive information.

iii. We have updated all our Data/Information Policies and informed all relevant parties affected – seeking refreshed consent where applicable.

iv. Training has been provided to all staff and to Carers Call volunteers.

v. Should, for any reason, there be dispute about how GDPR affects the processes of Carers Link or the rights of an individual – or if there is lack of detail within the policy section – Carers Link will be guided by the ICO Guide to GDPR and its contents will supersede any content of our Information Policies:
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

10. Right to Access

iii. Any Carer, Volunteer, Student or Staff Member can access information on them held by Carers Link at any time.

iv. When requesting your personal information it is preferred that they please contact the CEO in writing including the following information:
- your full name, address and contact telephone number
- any information to identify or distinguish you from others of the same name (e.g. date of birth);
- details of the **specific** information you require and any relevant dates

v. Nevertheless, we are aware that subject access requests may also be made verbally and to any member of staff, who should alert the CEO or Office Manager immediately.

vi. Please also note that you are however only entitled to access information directly related to you. Should the information requested contain information that relates to another person (including staff and volunteers), Carers Link is entitled to remove this information before sharing unless express permission is given for it to be released.

vii. Carers Link will respond to your request within 30 days starting from the day we receive details of the information we need to identify you and details of the information requested.

viii. Young people also have the right to access their own records but no one else's. Information will be made available to them in an age-appropriate form and should avoid causing them harm.

ix. Parents may only access their child's records if:
- The young person is under the age of 12 **OR**
- The young person is 12 or over **and** gives their consent **OR**
- The child cannot make a competent, informed choice **but** sharing the information is in the child's best interests.

x. More detailed information on access to records is available within the policies for that group i.e. carers, young carers, staff and volunteers.

11. Right to Rectification

i. Carers Link will respect the right of staff, volunteers and carers to rectify any incorrect information that may be held about them.

ii. In some circumstances, this may be straightforward and will simply be an up-dating of the information held e.g. phone number or address, in which case, Carers Link will comply with the request as soon as it is practical to do so but certainly within 30 days.

iii. If however, the request is to rectify an opinion, this becomes more complex. Opinions are, by their very nature, subjective, and it can be difficult to conclude that the record of an opinion is inaccurate. As long as the record shows clearly that the information is an opinion and, where appropriate, whose opinion it is, it may be difficult to say that it is inaccurate and needs to be rectified.

iv. In such situations, we will investigate the information held and speak to the processor and any other staff involved. We will then either let the record stand or amend as requested.

v. If we are satisfied that the personal data is accurate, we will inform that we will not be amending the data and why. We will also inform of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

vi. We will however, also place a note on the record indicating that the individual challenges the accuracy of the data and their reasons for doing so.

12. Right to Object/Restrict Processing

i. Individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

ii. As such, all newsletters and e-bulletins will be circulated via Mail Chimp and contain opportunity to state that the recipient wishes to opt-out of future receipt.

iii. Any such requests should have their Consent/Marketing Preferences updated on Charity Log and communication options suppressed as required.

iv. If, however the data is being processed under Vital Interest, Contract or Legal Obligation, there is no right to objecting to the data being processed.

v. If the data is being processed under 'Legitimate Interests', the individual should inform of their reasons why the personal or sensitive data should no longer be processed. Carers Link will then need to weigh these reasons against our own reasons for processing the information.

vi. At all times, the carer will be informed of the outcome and our justifications on the rare occasion that we need to continue processing. We will also inform of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

13. Right to Data Portability

i. The right to data portability gives individuals the right to receive personal data they have provided to Carers Link. It also gives them the right to request that Carers Link transmits this data directly to someone in another organisation who has responsibility for Data Protection i.e. a Data Controller.

ii. An example of this use may be a carer moving to another local authority or seeking support from another organisation. It may also be utilised in caring situations that cross boundaries.

iii. Information is only within the scope of the right to data portability if it is personal data of the individual that they have provided to Carers Link and if this information is in an automated/electronic format.

iv. The information to be transferred has to be in a format that is structured; commonly used; and machine-readable. An example of this will be use of excel/csv spreadsheets.

v. Should we receive information through the Right to Data Portability, the Data Controllers will
   - Consider whether it is relevant and/or excessive
   - Check it for third-party details

- Decide the lawful basis for processing it

vi. Any information received that we do not require will be deleted.

14. Right to Erasure / 'To Be Forgotten'

i. Individuals have the right to have their personal data erased if:
   - The personal data is no longer necessary for the purpose which you originally collected or processed it for;
   - The lawful basis for holding the data is 'Consent', and the individual withdraws their consent;
   - The lawful basis for holding the data is 'Legitimate Interests', the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
   - The personal data is being used for direct marketing purposes and the individual objects to that processing;
   - The personal data has been processed unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
   - Carers Link has to comply with a legal obligation; or
   - Carers Link has processed the personal data to offer information society services to a child.

ii. There are a number of reasons why this right may not apply, however in particular the right to erasure does not apply if Carers Link is processing data to comply with legal obligations or for statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or for the establishment, exercise or defence of legal claims.

iii. Please note that Carers Link requires holding carer records for a period of 7 years.

iv. Any requests, verbal or written, should be immediately passed to either Data Controller.

v. At all times, the carer will be informed of the outcome and our justifications should we need to continue processing. We will also inform of their right to make a complaint to the ICO or another supervisory authority; and their ability to seek to enforce their rights through a judicial remedy.

15. Automated Decision Making

i. Carers Link does not envisage that any decisions will be taken about staff, volunteers or carers using automated means, however individuals will be notified if this position changes.

C. Data Breaches

i. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

ii. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

iii. Personal data breaches can therefore include:
   - Access by an unauthorised third party;
   - Deliberate or accidental action (or inaction) by a controller or processor (i.e. staff, student or volunteer);
   - Sending personal data to an incorrect recipient;
   - Computing devices containing personal data being lost or stolen;
   - Alteration of personal data without permission; and
   - Loss of availability of personal data.

iv. On becoming aware of a breach, Carers Link will try to contain it or recover information affected. We will then assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

v. Carers Link will be guided in our assessment using:
   - https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

vi. Carers Link will document all and any breaches in data protection, in line with GDPR – even if it is not deemed as being reportable to either the ICO and/or an individual or individuals. This will include documenting the facts relating to the breach, its effects and the remedial action taken.

vii. Responsibility for documenting breaches will lie with the Data Controllers; however responsibility for subsequent actions will depend on the severity and effect of the breach. This will include (but not be limited to) Data Controllers taking action (or taking no further action) after consultation:
   - With each other
   - With members of the Management Team
   - With members of the Board of Management

D. Special Categories

16. Information relating to Young People

i. Young people have the same rights as adults under GDPR and therefore the contents of this policy apply equally to young persons as to adults. Nevertheless, there are some additional aspects to be considered below.

ii. A specific policy and information leaflet 'Wheesht' has been designed and made available to young people involved in the organisation. It is also available on our website.

iii. Carers Link is committed to providing a safe environment for young people and recognises that trust is essential for good youth work and is the foundation for all relationships within the Linkedup Service. Maintaining confidences is an integral part of building trust between young people, staff, volunteers and the organisation and will be respected at all times, apart from where it conflicts with reporting child protection concerns.

iv. Young people can expect that any information they give to a worker is treated as sensitive and confidential and will not be shared unless:

v. The worker believes that the young person, or another young person, is in danger or is being harmed. In this case the young person will be told that the information has to be shared with the appropriate agencies and encouraged to agree with this.

vi. The young person discloses that they are involved, or plan to become involved in acts of terrorism or other crime.

vii. Young people have the right to access their own records but no one else's. Information should be made available to them in an age-appropriate form and should avoid causing them harm.

viii. Parents may only access their child's records if
   - The young person is 12 or over **and** gives their consent **OR**
   - The child cannot make a competent, informed choice **but** sharing the information is in the child's best interests.

17. Specific Guidance on PVG & Disclosure Data

ix. Carers Link complies fully with the Code of Practice, issued by Scottish Ministers, regarding the correct handling, holding and destroying of Disclosure information provided by Disclosure Scotland under Part V of the Police Act 1997, for the purposes of assessing applicants' suitability for positions of trust.

x. We use Disclosure Information and Records through the Protecting Vulnerable Group (PVG) Scheme only for the purpose for which they have been provided.

xi. The PVG Scheme Record and Disclosure information provided by an individual for a position within Carers Link is not used or disclosed in a manner incompatible with the purpose.

xii. Carers Link recognises that, under section 124 of the Police Act 1997, it is a criminal offence to disclose PVG Scheme Record and Disclosure Information to any unauthorised person. We, therefore, only pass Disclosure Information to those who are authorised to see it in the course of their duties, namely the CEO, the Office Manager, Management Team, Board of Directors Staffing sub-group (if applicable), and – only with regard to Disclosures of Volunteers – the Volunteers Co-ordinator.

xiii. Carers Link will not disclose information provided under section 115(8) of the Act, namely information, which is not included in the Disclosure, to the applicant.

xiv. We do not keep PVG Scheme Record and Disclosure Information, other than the record or membership number, on any individual's personnel file. It is kept securely, in a locked filing cabinet within the office of the CEO for the period of any decision making processes. Access is strictly controlled to authorised and named individuals, namely the CEO and Office Manager who are required to see such information in the course of their duties.

xv. We do not keep PVG Scheme Record and Disclosure or PVG Scheme Record and Disclosure Information for any longer than is required after a recruitment (or any other relevant) decision has been taken. In general, this is no longer than 90 days. This is to allow for the resolution of any disputes or complaints.

xvi. PVG Scheme Record and Disclosure Information will only be retained for longer than this period in exceptional circumstances, and in consultation with Disclosure Scotland. The same conditions relating to secure storage and access will apply during any such period.

xvii. Details are, however, kept of the unique reference number of the PVG Scheme Record and Disclosure, the name of the subject and the date submitted. This is required for future Protecting Vulnerable Group Scheme Requests. This information is stored on the database.

xviii. Once any retention period has elapsed, we will ensure that PVG Scheme Record and Disclosure Information are immediately destroyed in a secure manner i.e. by shredding.

xix. Carers Link will not keep PVG Scheme Record and Disclosure Information, which is awaiting destruction in any insecure receptacle (e.g. a waste bin or confidential waste sack). We will not retain any image or photocopy or any other form of the Disclosure Information.

18. Policy Review

i. This Policy will be reviewed annually or as appropriate and in accordance with legislation.

Date	Activity	Date	Activity
June 2015	Policy Created		Choose an item.
January 2017	Reviewed Only		Choose an item.
May 2018	Reviewed & Updated		Choose an item.
	Choose an item.		Choose an item.
	Choose an item.		Choose an item.
	Choose an item.		Choose an item.
	Choose an item.		Choose an item.
	Choose an item.		Choose an item.
	Choose an item.		Choose an item.