**Personal Data Protection Policy**

**For Staff and Volunteers**

**(Issue 5 dated July 2021)**

**Compliance with the**

**General Data Protection Regulation**

**(GDPR)**

|  |  |  |
| --- | --- | --- |
| **Issue** | **Date** | **Details** |
| 1 | May 18 | Initial Document |
| 2 | Sep 18 | Reformat for greater clarity including improved legal base(s) description. |
| 3 | July 19 | Reviewed and reformatted into standard ACG font with some minor amendments |
| 4 | Jan 21 | Organisation trading name changed throughout |
| 5 | Jul 21 | Organisation name changed throughout |
|  |  |  |
|  |  |  |

**You must read this policy because it gives important information about:**

• the data protection principles with which Later Life Choices Glenrothes (LLCG) must comply;

• what is meant by personal information (or data) and sensitive personal information (or data);

• how LLCG gathers, uses, stores and (ultimately) deletes personal information and sensitive personal information in accordance with the data protection principles;

• where more detailed privacy information can be found, e.g. about the personal information gathered and used about individuals, how it is used, stored, who it is shared with, for what purposes, the steps taken to keep that information secure, and for how long it is kept.

• your rights and obligations in relation to data protection; and

• the consequences of failure to comply with this policy.

Once you have read and understood this policy, please confirm you that have done so by signing and returning the attached copy to the Centre Manager.

Table of Contents

Contents

[Contents 3](#_Toc10208513)

[Introduction 4](#_Toc10208514)

[2. Scope 4](#_Toc10208515)

[3. Definitions 5](#_Toc10208516)

[4. Data Protection Principles 5](#_Toc10208517)

[5. Basis for Processing Personal Information 6](#_Toc10208518)

[6. Sensitive Personal Information 6](#_Toc10208519)

[7. Criminal Records Information 8](#_Toc10208520)

[8. Data Protection Impact Assessments (DPIAs) 8](#_Toc10208521)

[9. Documentation and Records 8](#_Toc10208522)

[10. Privacy Notices 9](#_Toc10208523)

[11. Individual Rights 9](#_Toc10208524)

[12. Individual Obligations 10](#_Toc10208525)

[13. Information Security 11](#_Toc10208526)

[14. Storage and Retention of Personal Information 12](#_Toc10208527)

[15. Data Breaches 12](#_Toc10208528)

[16. Training 13](#_Toc10208529)

[17. Consequences of Failing to Comply 13](#_Toc10208530)

[Annex A - The Lawful Bases for processing personal data at LLCG 15](#_Toc10208531)

[Annex B - List of LLCG Policy Documents Relevant to Personal Data Protection 21](#_Toc10208532)

[Annex C – LLCG Privacy Notice 22](#_Toc10208533)

Introduction

* 1. Later Life Choices Glenrothes (LLCG) takes the security and privacy of personal information seriously. LLCG gathers, uses and stores data about you and others in the normal course of its business and the delivery of its services and to manage its relationship with you and others with whom it has dealings and comes into contact with. LLCG has a duty to notify you of the information contained in this Policy.
  2. LLCG obtains, uses, and stores personal information (also referred to as data), as set out in LLCG's Privacy Notices, for a number of specific lawful purposes, about job applicants, current staff, temporary workers, volunteers, suppliers, clients, carers, partners, funders and any other third parties the organisation has dealings with.
  3. This policy sets out how LLCG complies with its data protection obligations and seeks to protect personal information relating to its workforce and others.
     1. Its purpose is also to ensure that staff, volunteers and others working with or for LLCG understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.
  4. LLCG is committed to complying with its data protection obligations, and to being concise, clear and transparent about how it obtains and uses personal information relating to its workforce and others, and how (and when) that information is deleted once it is no longer required.
  5. The Centre Manager is responsible for data protection compliance within LLCG. If you have any questions or comments about the content of this policy or if you need further information, you should contact them on [info@laterlifechoicesglenrothes.org](mailto:info@laterlifechoicesglenrothes.org).

1. Scope
   1. This policy applies to the personal information of staff and volunteers as identified at paragraph 1.2 above.
   2. Staff and volunteers should refer to LLCG's Privacy Notice (attached at Annex C) and, where appropriate, to its other relevant policies including in relation to internet, e-mail and communications, monitoring, social media, information security, data retention, and criminal record information. These contain further information regarding the protection of personal information in those contexts. A list of the relevant LLCG policy documents is shown at Annex B.
   3. LLCG will review and update this policy in accordance with its data protection obligations. It does not form part of any staff member’s contract of employment and LLCG may amend, update or supplement it from time to time. Any new or modified policy will be circulated to staff [and volunteers] before it is adopted.
2. Definitions

|  |  |
| --- | --- |
| **criminal records information** | means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures; |
| **data breach** | means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information; |
| **data subject** | means the individual to whom the personal information relates; |
| **personal information** | (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information; |
| **processing information** | means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it; |
| **pseudonymised** | means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual; |
| **sensitive personal information** | (sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual), and information concerning an individual's health, sex life or sexual orientation. |

1. Data Protection Principles
   1. LLCG will comply with the following data protection principles when processing personal information:
      1. process personal information lawfully, fairly and in a transparent manner;
      2. collect personal information for specified, explicit and lawful purposes only, and will not process it in a way that is incompatible with those purposes; the legal bases for LLCG’s collecting and processing personal data are described at Annex A.
      3. only process the personal information that is adequate, relevant and necessary for LLCG to provide its service;
      4. keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
      5. keep personal information in a form which permits identification of data subjects

for no longer than is necessary for the purposes for which the information is processed; and

* + 1. take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

1. Basis for Processing Personal Information
   1. In relation to any processing activity LLCG will, before the processing starts for the first time, and then regularly while it continues:
      1. review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:
         1. that the data subject has consented to the processing;
         2. that the processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;
         3. that the processing is necessary for compliance with a legal obligation to which LLCG is subject;
         4. that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
         5. that the processing is necessary for the purposes of legitimate interests of LLCG or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject-see clause 5.2 below.
      2. except where the processing is based on consent, ensure that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
      3. document its decision as to which lawful basis applies to help demonstrate compliance with the data protection principles;
      4. include information about both the purposes of the processing and the lawful basis for it in its relevant Privacy Notice(s);
      5. where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 6.2.2 below), and document it; and
      6. where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.
      7. The lawful bases for the collection and processing of personal data at LLCG are detailed at Annex A.
2. Sensitive Personal Information
   1. Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.
   2. LLCG may from time to time need to process sensitive personal information. The organisation will only process sensitive personal information if:
      1. it has a lawful basis for doing so as set out in paragraph 5.1.1 above, e.g. it is necessary for the performance of the employment contract, to comply with LLCG's

legal obligations, or for the purposes of LLCG's legitimate interests; and

* + 1. one of the special conditions for processing sensitive personal information applies, i.e.:
       1. the data subject has given explicit consent;
       2. the processing is necessary for the purposes of exercising the employment law rights or obligations of LLCG or the data subject;
       3. the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
       4. processing relates to personal data which are manifestly made public by the data subject;
       5. the processing is necessary for the establishment, exercise or defence of legal claims; or
       6. the processing is necessary for reasons of substantial public interest.
  1. Before processing any sensitive personal information, staff must notify the Centre Manager of the proposed processing, in order that they may assess whether the processing complies with the criteria noted above.
  2. Sensitive personal information will not be processed until:
     1. the assessment referred to in paragraph 6.3 has taken place; and
     2. the individual has been properly informed (by way of a Privacy Notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.
  3. LLCG will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.
  4. Where appropriate, LLCG's Privacy Notices set out the types of sensitive personal information that LLCG processes, what it is used for and the lawful basis for the processing.
  5. In relation to sensitive personal information, LLCG will comply with the procedures set out in paragraphs 6.8 and 6.9 below to make sure that it complies with the data protection principles set out in paragraph 4 above.
  6. During the recruitment process LLCG will ensure that (except where the law permits otherwise):
     1. during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g. race or ethnic origin, trade union membership or health;
     2. if sensitive personal information is received, e.g. the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;
     3. any completed equal opportunities monitoring form is kept separate from the individual's application form, and not seen by the person short-listing, interviewing or making the recruitment decision;
     4. 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;
     5. health questions will only be asked once an offer of employment has been made.
  7. During employment LLCG will process:
     1. health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits; and
     2. sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting. Where possible, this information will be anonymised;

1. Criminal Records Information
   1. Where criminal records information requires to be process, LLCG will process it in accordance with the data protection principles.
2. Data Protection Impact Assessments (DPIAs)
   1. Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the organisation is planning to use a new form of technology), LLCG will, before commencing the processing, carry out a DPIA to assess:
      1. whether the processing is necessary and proportionate in relation to its purpose;
      2. the risks to individuals; and
      3. what measures can be put in place to address those risks and protect personal information.
   2. Before any new form of technology is introduced, the Centre Manager should carry out a DPIA.
   3. During the course of any DPIA, the Centre Manager will seek the advice of the Data Protection Adviser (board member).
3. Documentation and Records
   1. LLCG will keep written records of processing activities which are high risk i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:
      1. the name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and person responsible for data protection);
      2. the purposes of the processing;
      3. a description of the categories of individuals and categories of personal data;
      4. categories of recipients of personal data;
      5. where relevant, details of transfers to countries out with the EEA, including documentation of the transfer mechanism safeguards in place;
      6. where possible, retention schedules; and
      7. where possible, a description of technical and organisational security measures.
   2. As part of LLCG’s record of processing activities it documents, or links to documentation, on:
      1. information required for privacy notices;
      2. records of consent;
      3. controller-processor contracts;
      4. the location of personal information;
      5. DPIAs; and
      6. records of data breaches.
   3. If LLCG processes sensitive personal information or criminal records information, it will keep written records of:
      1. the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
      2. the lawful basis for its processing; and
      3. whether it retains and erases the personal information in accordance with its policy document and, if not, the reasons for not following its policy.
   4. LLCG will conduct regular reviews of the personal information it processes and update its documentation and policies accordingly.
4. Privacy Notices
   1. LLCG will issue Privacy Notices from time to time, informing people about the personal information that it collects and holds relating to them and others (third parties) (e.g. volunteers, clients, carers), how they can expect their personal information to be used (and for what purposes), and where appropriate, how staff/volunteers are expected to process third parties' personal information.
   2. LLCG will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
5. Individual Rights
   1. You (in common with other data subjects) have the following rights in relation to your personal information:
      1. to be informed about how, why and on what basis that information is processed;
      2. to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request-

see LLCG's information on subject access request;

* + 1. to have data corrected if it is inaccurate or incomplete;
    2. to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
    3. to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and
    4. to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether LLCG's legitimate grounds override your interests).
  1. If you wish to exercise any of the rights in paragraphs 11.1.3 to 11.1.6, please contact the Centre Manager.

1. Individual Obligations
   1. Individuals are responsible for helping LLCG keep their personal information up to date. You should let the Centre Manager know if the information you have provided to LLCG changes, for example if you move to a new house or change details of the bank or building society account to which you are paid.
   2. You may have access to the personal information of other members of staff, volunteers, clients, carers, suppliers, partners or funders to LLCG in the course of your employment or arrangements with LLCG. If so, LLCG expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 11.1 above.
   3. If you have access to personal information, you must:
      1. only access the personal information that you have authority to access, and only for authorised purposes;
      2. only allow other staff or volunteers from LLCG to access personal information if they have appropriate authorisation;
      3. only allow individuals who are not staff or volunteers from LLCG to access personal information if you have specific authority to do so from the Centre Manager;
      4. keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in LLCG's relevant policies;
      5. not remove personal information, or devices containing personal information (or which can be used to access it), from LLCG's premises unless appropriate security measures are in place (such as pseudonymisation, encryption and/or password protection) to secure the information and/or the device; and
      6. not store personal information on local drives or on personal devices that are used for work purposes and you must comply with LLCG's Internet, Email & Social Media Policy.
   4. You should contact the Centre Manager if you are concerned or suspect that one of the following has taken place (or is taking place or is likely to take place):
      1. processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 6.2.b being met;
      2. any data breach as set out in paragraph 16.1 below;
      3. access to personal information without the proper authorisation;
      4. personal information not kept or deleted securely;
      5. removal of personal information, or devices containing personal information (or which can be used to access it), from LLCG's premises without appropriate security measures being in place;
      6. any other breach of this policy or of any of the data protection principles set out in paragraph 4.1 above.
2. Information Security
   1. LLCG will use appropriate technical and organisational measures in accordance with its policies on information security to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:
      1. making sure that, where possible, personal information is pseudonymised or encrypted;
      2. ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
      3. ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
      4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
   2. Where LLCG uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:
      1. the external organisation may act only on the written instructions of LLCG;
      2. those processing the data are subject to a duty of confidence;
      3. appropriate measures are taken to ensure the security of processing;
      4. sub-contractors are only engaged with the prior consent of LLCG and under a written contract;
      5. the external organisation will assist LLCG in providing subject access and allowing

individuals to exercise their rights in relation to data protection;

* + 1. the external organisation will assist LLCG in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
    2. the external organisation will delete or return all personal information to LLCG as requested at the end of the contract; and
    3. the external organisation will submit to audits and inspections, provide LLCG with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell LLCG immediately if it is asked to do something infringing data protection law.
  1. Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Centre Manager.

1. Storage and Retention of Personal Information
   1. Personal information (and sensitive personal information) will be kept securely and for no longer than necessary in accordance with LLCG's Personal Data Storage & Retention Policy.
   2. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow LLCG's Personal Data Storage & Retention Policy which sets out the relevant retention periods for a variety of data. Where there is any uncertainty, staff should consult the Centre Manager.
   3. Personal information (and sensitive personal information) that is no longer required will be deleted permanently from LLCG’s information systems and any hard copies will be destroyed securely.
2. Data Breaches
   1. A data breach may take many different forms, for example:
      1. loss or theft of data or equipment on which personal information is stored;
      2. unauthorised access to or use of personal information either by a member of staff or third party;
      3. loss of data resulting from an equipment or systems (including hardware and software) failure;
      4. human error, such as accidental deletion or alteration of data;
      5. unforeseen circumstances, such as a fire or flood;
      6. deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
      7. 'blagging' or social engineering offences, where information is obtained by deceiving the organisation which holds it.
   2. LLCG will:
      1. make the required report of a data breach to the Information Commissioner's

Office without undue delay and, where possible, within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

* + 1. notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.
  1. Information may be held at LLCG’s offices and third-party agencies, service providers, representatives and agents. Information may be transferred outside the European Economic Area (EEA) (which comprises countries in the European Union and Iceland, Liechtenstein and Norway) to countries that do not have data protection laws equivalent to those in the UK. Such countries and/or organisations are designated as having an adequate level of protection. LLCG has security measures in place to seek to ensure that there is appropriate security for information it holds.

1. Training
   1. LLCG will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.
2. Consequences of Failing to Comply
   1. LLCG takes compliance with this policy very seriously. Failure to comply with the policy:
      1. puts at risk the individuals whose personal information is being processed;
      2. carries the risk of significant civil and criminal sanctions for the individual and LLCG; and
      3. may, in some circumstances, amount to a criminal offence by the individual.
   2. Due to the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under LLCG’s procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract or, in the case of volunteers their volunteer agreement, terminated with immediate effect.
   3. If you have any questions or concerns about anything in this policy, do not hesitate to contact the Centre Manager.
   4. Once you have read this document you must sign off against the ‘Personal Data Protection Policy’ on your ‘Training – Policies’ record held on your personnel file/volunteer file. This is to show you have read, understood and will comply with this policy. Contact the Centre Manager for access to your ‘Training-Policies’ record.

Annexes (attached)

A. The lawful bases for the collection and processing of personal data at LLCG.

B. List of LLCG Policy Documents Relevant to Personal Data Protection

C. LLCG Privacy Statement

Annex A - The Lawful Bases for processing personal data at LLCG

1. **The GDPR Options**
   1. In relation to any personal data processing activity an organisation must review the purposes of the particular processing activity, and select from the following six options the most appropriate lawful basis (or bases) for that processing:
      1. **Consent**. The individual has opted in and consented to having his or her personal information processed.
      2. **Contractual Obligation**. It is necessary to process the personal data to fulfil your contract or pre-contractual obligations.
      3. **Legal Obligation**. It is necessary to process the personal data to fulfil a legal obligation.
      4. **Vital Interests**. It is necessary to process the personal data to protect the vital interest of the individual or another individual.
      5. **Public Task**. It is in the exercise of official authority or within the public’s interest to process the personal data.
      6. **Legitimate Interests**. Processing of the personal data is necessary under the Legitimate Interests of the Data Controller or Third Party, unless these interests are overridden by the individual’s interests or fundamental rights.
   2. In particular LLCG must:
      1. Except where the processing is based on consent, satisfy itself that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
      2. Document its decision as to which lawful basis applies, to help demonstrate its compliance with the data protection principles;
      3. Include information about both the purposes of the processing and the lawful basis for it in its relevant Privacy Notice(s);
      4. Where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.
2. **LLCG’s Legal Basis for Processing Personal Data**
   1. LLCG collects personal data from four groups of people: staff, volunteers (including the Board), clients and family members of clients.
   2. **Staff**. This grouping is characterised by being paid, on contract, directly involved with vulnerable adults and volunteers, subject to LLCG’s employment regulations.
      1. Lawful Basis: LLCG needs to process staff personal data to fulfil its contractual obligations to them and to ensure they are fit to support vulnerable adults. LLCG cannot fulfil its responsibilities to them without this processing.
      2. Therefore, LLCG will rely on **CONTRACTUAL OBLIGATION** as the lawful basis for processing the personal data of staff.

| **The Information LLCG collects from Staff** | **Why LLCG collects the information & what it is used for** | **Duration of Processing** |
| --- | --- | --- |
| * Full Name * Title * Address * Tel No (home/mobile) * Email address * Right to work in UK * Info on disability/health issues/support needs * Academic qualifications * Other relevant qualifications * Previous employers’ info * Referees’ x 2 contact details and signature * Criminal Convictions (including ‘spent’) * Place of Birth * Date of birth * Signature * Mother’s maiden name * Gender * Town & country of birth * Nationality * ID (photographic such as passport/driving licence or birth certificate plus 2 to 3 official letters showing proof of current address * 5 year address history * Regulatory Body codes (if applicable) * Copy of PVG Membership application form * PVG Membership number * LLCG Job Title * Start Date * Annual salary * Hours of work * Copy of driving licence (if applicable) * Copy of motor insurance (if applicable) * Copy of DVLA Licence Summary (if applicable) * NI number * Next of Kins’ details x 2 – name, address, relationship, home /mobile/ work telephone numbers * Bank Details – account name, sort code, account number, name of bank * Tax Info * Auto Enrolment Pension Info * Photograph * Copies of training Certificates * Sickness/absence records * Supervision / Disciplinary records * Copies of payslips * Timesheets (Daily Logs) * Annual Leave/ TOIL records * Exit Interview form * Leaving Date | * to recruit new staff members * to undertake background checks via the PVG Scheme * to meet contract of employment * to ensure suitability for driving if part of role * to ensure LLCG can contact staff members’ NOK in an emergency * to calculate payroll and to provide details to staff members, HMRC, pension provider(s) and other statuary bodies as required by law * to make a photographic ID badge for staff members * to provide support to staff members in line with LLCG’s policies such as Absence Management Policy and Staff Support & Supervision policies * general ongoing employment purposes | * all information held for **6 months** after staff members cease employment with the following exceptions:      * unsuccessful recruitment applications at end of process; * copy of PVG Membership application on receipt of PVG certificate; * ID badge on leaving * contact details on website as soon as possible after leaving * individual email account one month after leaving * daily logs **2 years** after leaving * any disciplinary records **6** **years** after leaving * any information relating to payroll **6 years** after leaving * any information relating to pension **6 years** after leaving * electronic information is deleted from LLCG’s network and hard copy information is shredded or is disposed of through confidential waste bags |

* 1. **Volunteers (including the Board)**. This grouping is characterised by being unpaid, not on contract, involved with vulnerable adults, subject to LLCG’s service regulations.
     1. Lawful Basis: LLCG needs to process volunteers’ personal data to support and communicate with them, and to ensure they are fit to support vulnerable adults. LLCG cannot fulfil its responsibilities to them without this processing.
     2. Therefore, LLCG will rely on **CONSENT** as the lawful basis for processing the personal data of volunteers.

| **The Information LLCG collects from Volunteers** | **Why LLCG collects the information & what it is used for** | **Duration of Processing** |
| --- | --- | --- |
| * Full Name * Title * Address * Tel No (home/mobile) * Email address * Info on disability/health issues/support needs * Relevant training/ skills * Referees’ x 2 contact details and signature * Criminal Convictions (including ‘spent) * Place of Birth * Date of birth * Signature * Mother’s maiden name * Gender * Town & country of birth * Nationality * ID (photographic such as passport/driving licence or birth certificate plus 2 to 3 official letters showing proof of current address * 5 year address history * Regulatory Body codes (if applicable) * Copy of PVG Membership application form * PVG Membership number * LLCG Volunteer Role * Start Date * Sessions/times volunteering at * Copy of driving licence (if applicable) * Copy of motor insurance (if applicable) * Copy of DVLA Licence Summary (if applicable) * Emergency Contact’s details – name, relationship, home /mobile/ work telephone numbers * GP’s name, surgery name, address, telephone number * Photograph * Copies of training Certificates * Disciplinary records * Reason for leaving * Leaving date | * to recruit new volunteers * to undertake background checks via the PVG Scheme * to meet terms of the volunteer agreement * to ensure suitability for driving if part of role * to ensure LLCG can contact volunteers’ NOK in an emergency * to provide support to volunteers in line with LLCG policies * general ongoing volunteering purposes | * all information held for **6 months** after volunteers cease volunteering with the following exceptions: * unsuccessful volunteer applications at end of process; * copy of PVG Membership application on receipt of PVG certificate; * ID badge on leaving * Name, role, start date, end date, PVG membership number, reason for leaving **2 years** after leaving * electronic information is deleted from LLCG’s network and hard copy information is shredded or is disposed of through confidential waste bags |

* 1. **Clients**. This grouping is characterised by being given a service by LLCG, contributing towards LLCG costs, and being vulnerable adults.
     1. Lawful Basis: LLCG needs to process clients’ personal data to support and communicate with them, and to understand any particular needs due to disability or frailty. Some clients suffer from the early onset of dementia who nevertheless are sufficiently aware to make informed consent. LLCG cannot fulfil its responsibilities to its clients without this processing.
     2. Therefore, LLCG will rely on **CONSENT** as the lawful basis for processing the personal data of clients.

| **The Information LLCG collects from Clients** | **Why LLCG collects the information & what it is used for** | **Duration of Processing** |
| --- | --- | --- |
| * Full Name * Known as * Diagnosis (and type) of dementia / other memory issues * Attendance at other centres / groups * Address * Telephone Number * Date of Birth * Referrer’s name, organisation, address, telephone number * Next of kin’s (NOK) name, address, telephone number * GP’s name, surgery * Referral reason (including disability/health issues and support needs * Emergency contact’s name, relationship, address, preferred method of contact, home phone, work phone, mobile, email address (could be same as NOK) * POA details if applicable * DNR details if applicable, including gender * Keyholder / keysafe number * Service(s) referred for * Info on continence/ mobility/ diet/ swallowing /food allergies/ vision/ hearing / speech / aid requirements for snack /other allergies or adverse reactions * Health support needs * Medication being brought to session * Any other support needs while attending * Transport requirements * Start Date * Signature * Photograph consent * Photograph for individual file * Third party involvement permission * Info on home circumstances, other support/ services, hobbies, likes, music taste, anything else client wishes to inform of * Reason for leaving * Leaving date | * to assess potential clients meet the criteria for LLCG services * to have sufficient knowledge about clients to deliver the most relevant service(s) * to keep clients safe and comfortable when receiving LLCG services * to support clients in a person-centred way * to tailor activities / services to clients’ preferences * to ensure LLCG can contact clients’ NOK/GP in an emergency | * all information held for **6 months** after client leaves LLCG service(s) * electronic information is deleted from LLCG’s network and hard copy information is shredded or is disposed of through confidential waste bags |

* 1. **Family Members (of Clients)**. This grouping is characterised by being the main family contact point for LLCG concerning individual clients.
     1. Lawful Basis: LLCG needs to process family members’ personal data to support and communicate with them and to understand any particular client needs. LLCG cannot fulfil its responsibilities to its clients without this processing.
     2. Therefore, LLCG will rely on **CONSENT** as the lawful basis for processing the personal data of family members.

| **The Information we collect from Client Family Members** | **Why LLCG collects the information & what it is used for** | **Duration of Processing** |
| --- | --- | --- |
| * Name * Address * Preferred method of contact * Home phone, work phone, mobile * Email address * Relationship to client * All/any of above client data if client has diagnosis of dementia / POA in place | * to have sufficient knowledge about clients to deliver the most relevant service(s) * to keep clients safe and comfortable when receiving LLCG services * to support clients in a person-centred way * to ensure LLCG can contact clients’ NOK in an emergency | * all information held for **6 months** after client leaves LLCG service(s) * electronic information is deleted from LLCG’s network and hard copy information is shredded or is disposed of through confidential waste bags |

1. **Sensitive Information**. Health, disability or criminal record information is deemed “sensitive” data and is collected only if considered necessary for the purposes of preventative or occupational measures to support the individual whilst associated with LLCG. No other sensitive data (as defined by the GDPR) is collected.

Annex B - List of LLCG Policy Documents Relevant to Personal Data Protection

1. Privacy Notice
2. Confidentiality Policy
3. Boundaries Policy
4. Personal Data Storage and Retention Policy
5. Data Breach Policy and Reporting
6. Training
7. Internet, Email and Social Media Policy
8. Data Processing Agreements
9. Subject Access Request Form

**Annex C - PRIVACY NOTICE**

**Later Life Choices Glenrothes (LLCG)**

(Issue 6, July 2021)

*Providing services for older people in and around Glenrothes which enhance their quality and enjoyment of life by encouraging interaction, mental & physical activity and companionship.*

**What is this Notice All About?**

LLCG collects and processes personal information about staff, volunteers, clients, and client family members so that it can provide the services needed. The General Data Protection Regulations (GDPR) 2018 gives individuals particular rights over the personal information given to organisations, so this notice introduces our privacy policy and lets you know how and why LLCG uses your personal information.

**A copy of our full personal data protection policy is available on our website** [**www.laterlifechoicesglenrothes.org**](http://www.laterlifechoicesglenrothes.org) **or in hard copy on request to the Centre Manager.**

*LLCG is committed to protecting your privacy by taking every reasonable effort to keep the personal information you give us secure and accurate.*

**The Later Life Choices Glenrothes Privacy Statement**

* Your personal information is only used for the purpose for which we collect it.
* Only information that we need is collected.
* Your personal information is only seen by those who need it to do their jobs.
* We will only disclose your personal information when we have your consent to do so or if we believe you are at risk of harm if we do not disclose it.
* We will keep your information up to date and will correct any inaccuracies as soon as possible.
* We will retain your personal information only for as long as it is needed to support the purpose for which it was collected. It will then be confidentially destroyed.
* We will protect your personal information from unauthorised or accidental disclosure and we will process it in a manner which maintains its integrity and confidentiality.
* We will provide you with a copy of your personal information on request

**What Information Do We Collect?**

The personal information we collect could include your name, photograph, address, email address, telephone number, date of birth, gender, relevant medical details (including any disability/support needs), next of kin, and (for employees of LLCG) bank details.

**What is LLCG’s Legal Basis for Collecting and Using Personal Information?**

Employed staff at LLCG are under contract, and therefore we have a contractual obligation to seek relevant personal information. Volunteers, clients and their family members are not under contract and so our seeking and using their personal information is on the basis of consent.

**Why Do We Collect This Personal Information And How Do We Use It?**

We collect this information to allow us to provide our services to you whilst you are associated with, or employed by, LLCG. For example, we need to be able to pay salaries to staff, to contact volunteers, clients and client family members, to provide transport services, or where possible to tailor our services to your needs.

**Who Has Access To Your Information?**

We will not allow anybody outside LLCG access to your information, except where we believe that sharing such information with health or social services professionals is necessary for your wellbeing. Under such circumstance we will always try to obtain your consent first.

**How Is My Information Stored and Protected?**

The information you give us will be stored on paper or electronically at 100 Scott Road. Paper information is held in an organised filing system under lock and key, and electronic information is held in password-protected computers. Back-ups of electronic information/data are held locally in a secure manner, and a further back up is held in on-line storage using password protection. All passwords are held securely and only divulged to those members of staff who need to know.

**How Long Do You Keep My Personal Information?**

Your data will be held only for as long as we need it to support your association with LLCG, after which time we will confidentially dispose of it unless required by law to keep it for a further period.

**What Are My Rights?**

You are entitled to view, amend, correct or delete the personal information that we hold. Please email or write to the LLCG Centre Manager if you wish to do so.You also have the right to complain to the Information Commissioner’s Office (ICO) if you think there is a problem with the way we are handling your data. The ICO’s contact details are:

The Information Commissioner's Office - Scotland

45 Melville Street

Edinburgh

EH3 7HL

Tel: 0303 123 1115

Email: [scotland@ico.org.uk](mailto:scotland@ico.org.uk)

**Who Can I Contact If I Have A Query?**

Any questions about this notice and our privacy practices should be sent in writing to: The Centre Manager, Later Life Choices Glenrothes, 100 Scott Road, Glenrothes, KY6 1AE (or email: fionak@laterlifechoicesglenrothes.org). LLCG’s data protection adviser at board level is Mr Rick Kiralfy, who can also be contacted through the Centre Manager if you have any further concerns or queries.

-------------------------------------------------------------------------------------------------------------------------------

**Agreement to permit Later Life Choices Glenrothes (LLCG) to collect and use your personal information**

I hereby authorise LLCG to collect and use my personal information as described above, and in line with its data protection policy.

I am happy for my personal information to be discussed with my nominated contact:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / shared with third parties as appropriate.

I **DO NOT** wish any personal information / matters to be discussed with any family member/ third party

Signed: ……………………………………………………………………………………………………………

Name: …………………………………………………………………………… Date: …………………………………………………