Data Protection Policy

This policy sets out our commitment to protecting personal data and how we will implement that commitment in our role as data controller.

Any queries relating to this policy should be sent to the CLC at privacy@clc-uk.org.

As a data controller the CLC is committed to:

- Ensuring data is processed fairly and lawfully;
- Ensuring personal data is processed only for specified and lawful purpose;
- Taking steps to ensure personal data is adequate and relevant to the purpose or purposes for which they are processed;
- Taking steps to ensure personal data is accurate and up to date;
- Ensuring personal data is only retained for a necessary period;
- Providing relevant parties (i.e. 'data subjects') with access to their data;
- Providing adequate security measures to protect personal data;
- Ensuring a nominated officer is responsible for data protection compliance;
- Providing adequate training for all staff responsible for personal data;
- Regularly reviewing data protection and guidelines within the CLC.

These commitments seek to ensure that we comply with the eight principles of the Data Protection Act 1998 as provided at the end of this policy. These commitments will be applied in the following manner:

Procuring data – as appropriate, we will issue notices, explaining to relevant individuals why we are gathering the data, obtaining their explicit consent where this is required, and advising them we will be the data controller for the purposes of the Act. No more data shall be collected than is necessary for the purpose(s) declared.

Safeguarding data – we will not hold data for longer than is necessary. In particular,

- Disclosure and Barring Service (DBS) certificates (previously CRB checks) obtained by the CLC will be securely deleted no later than 3 months after they have been received unless it is satisfied that there are regulatory reasons (such as a disciplinary investigation) not to do so. Such certificates will be securely deleted no later than 3 months after any such regulatory reason has ceased to apply; and
- Diversity profiling survey responses will be securely deleted after 3 months.

Where data has been earmarked for destruction, appropriate measures are taken to ensure that the data cannot be reconstructed and processed by third parties. Adequate measures are taken to safeguard data so as to minimize the risk of loss, destruction or unauthorised disclosure. CLC employees will not disclose any information about any relevant individual parties unless they are clear they have the appropriate authority to do so. Personal data will not be disclosed to public authorities unless that disclosure has been authorised by the CLC's Data Protection Officer.

Unlawful obtaining or disclosure of personal data or any other breach of section 55 of the Data Protection Act 1998 by CLC staff will be treated seriously and may lead to disciplinary action, up to, and including dismissal.

Processing data - Management Information Systems used to procure and process the data are reviewed to ensure they are as secure as possible. Personal data will not be processed except for the purpose(s) for which they were obtained or for a similar, analogous purpose. If the new purpose is very different, we will obtain consent from the relevant party. Individual parties have the right to object to their data being processed, or conversely being deleted.

Transferring and disclosing data – we will not transfer or disclose personal data outside the CLC except with the relevant party's consent or after consultation with the CLC's Data Protection Officer or another senior officer of the CLC where it is reasonably concluded that such transfer of disclosure is permitted in the public interest.

Accessing data – we are committed to facilitating the access of relevant parties to their own personal data, while bearing in mind the need to protect other individuals' rights of privacy. An individual making a subject access request will be required to complete a Subject Access request form available from the CLC website. The request will be determined by or with the authority of the Data Protection Officer, or, in his absence, by another senior officer of the CLC. The applicant will need to submit supporting documentation which establishes that they are relevant party and the data refers to them. The fee for a subject access request is £10.

The Data Protection Principles

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under the Act;
7. Appropriate technical and organisational measures shall be taken against unauthorised and unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data