Data Protection and Confidentiality Policy

Responsible Manager	**Director of Finance**
Date of Issue	**May 2016**
Issue Number	**V2.0**
Date for Review	**May 2018**

Table of Contents

1 Policy Statement

1.1 This policy sets out the obligations of CXK Ltd ("the Charity") with regard to data protection and the rights of individuals ("data subjects") in respect of their personal data under the Data Protection Act 1998 ("the Act"). Under the Act, "personal data" is defined as data which relates to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller (the Charity in this context), and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

1.2 This policy sets out the procedures that are to be followed when dealing with personal data. The procedures set out herein must be followed at all times by the Charity, its employees, agents, contractors, or other parties working on behalf of the Charity. Failure to do so may result in disciplinary action.

1.3 The Charity is committed not only to the letter of the law but also to the spirit of the law and places a high premium on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals.

1.4 The Charity is registered with the Information Commissioner as a data controller under the register number Z679996X which is held by the Information Commissioner pursuant to Section 19 of the Act.

2 Aims and Objectives

2.1 This policy is set out to identify how the Charity executes its duty to keep personal information safe and confidential whilst at the same time not compromising its ability to share information where it is needed.

2.2 The purpose of this policy is to lay down the principles that must be observed by all who work within the Charity, including volunteers who have access to personal information.

2.3 The Charity is committed to maintaining the confidentiality of personal information that it handles. Any information given or received in confidence for one purpose will not be used for another purpose or passed to a third party, without their consent except in special circumstances (e.g. to prevent harm to an individual).

2.4 The Charity will ensure that personal information is obtained, used and disclosed in accordance with the common law duty of confidentiality and the Act.

2.5 The Charity will also have full regard for current and future legal requirements which impinge on the confidentiality of personal information in general, and specific categories of personal information.

3 About This Policy

3.1 The types of personal data that the Charity may be required to handle include information about current, past and prospective clients, suppliers and others that we communicate with. The personal data, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Act and other regulations.

3.2 This policy and any other documents referred to in it sets out the basis on which we will process any personal data we collect from data subjects, or that is provided to us by data subjects or other sources.

3.3 This policy does not form part of any employee's contract of employment and the Charity reserve the right to amend it at any time.

3.4 This policy has been approved by the Board It sets out rules on data protection and the legal conditions that must be satisfied when we obtain, handle, process, transfer and store personal data.

3.5 The Data Protection Officer is responsible for ensuring compliance with the Act and with this policy. That post is held by:

Gavin Maynard: gavin.maynard@cxk.org.uk - 07798632083

3.6 Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer.

4 Definition of Data Protection Terms

4.1 Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

4.2 Data subjects for the purpose of this policy include all living individuals about whom the Charity holds personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

4.3 Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

4.4 Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with the Act. We are the data controller of all personal data used in our business for our own purposes.

4.5 Data users are those of our employees whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

4.6 Data processors include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions. Employees of data controllers are excluded from this definition but it could include suppliers and agencies which handle personal data on the Charity's behalf.

4.7 Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

4.8 Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, including a condition requiring the express permission of the person concerned.

5 Data Protection Principles

5.1 Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

a) Processed fairly and lawfully.

b) Processed for limited purposes and in an appropriate way.

c) Adequate, relevant and not excessive for the purpose.

d) Accurate.

e) Not kept longer than necessary for the purpose.

f) Processed in line with data subjects' rights.

g) Secure.

h) Not transferred to people or organisations situated in countries without adequate protection.

6 Fair and Lawful Processing

6.1 The Act is 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. Any and all personal data collected by the Charity is collected in order to ensure that the Charity can provide the best possible service to its clients, and can work effectively with its partners, associates and affiliates and efficiently manage its employees, contractors, agents and consultants. The Charity may also use personal data in meeting certain obligations imposed by law.

6.2 The right to object to any processing of his or her personal data that is likely to cause (or that is causing) damage or distress. Data subjects should make any such objection in writing to the Data Protection Officer, and the Charity shall respond within 21 days either notifying the data subject of its compliance, or explaining why the Charity feels that any aspect of the data subject's request is unjustified.

- The right to prevent processing for direct marketing purposes.
- The right to object to decisions being taken by automated means (where such decisions will have a significant effect on the data subject) and to be informed when any such decision is taken (in which case the data subject has the right to require the data controller (by written notice) to reconsider the decision.
- The right to have inaccurate personal data rectified, blocked, erased or

destroyed in certain circumstances.

- The right to claim compensation for damage caused by the Charity's breach of the Act.

6.3 In particular, the Charity shall ensure that:

- All personal data collected and processed for and on behalf of the Charity by any party is collected and processed fairly and lawfully.
- Data subjects are always made fully aware of the reasons for the collection of personal data and are given details of the purpose(s) for which the data will be used.
- Personal data is only collected to the extent that is necessary to fulfil the purpose(s) for which it is required.
- All personal data is accurate at the time of collection and kept accurate and up to date while it is being held and/or processed.
- No personal data is held for any longer than necessary in light of the purpose(s) for which it is required.
- All personal data is held in a safe and secure manner, taking all appropriate technical and organisational measures to protect the data.
- All personal data is transferred securely, whether it is transmitted electronically or in hard copy.
- No personal data is transferred outside of the European Economic Area (as appropriate) without first ensuring that the destination country offers adequate levels of protection for personal data and the rights of data subjects.
- All data subjects can fully exercise their rights with ease and without hindrance.

7 Accurate Data

7.1 We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

8 Timely Processing

8.1 We will not keep personal data longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all data which is no longer required, but taking into account our legal obligations.

9 Data Security

9.1 We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

9.2 We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

9.3 We will maintain data security by protecting the confidentiality, integrity and availability of the personal data. Security procedures include:

a) Entry controls. Any stranger seen in entry-controlled areas should be reported.

b) Secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential).

c) Methods of disposal. Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required.

d) Equipment. Data users must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

10 Disclosure and Sharing of Personal Information

10.1 We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding and its subsidiaries, as defined in section 1159 of the UK Companies Act 2006.

10.2 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.

11 Access by Data Subjects

11.1 A data subject may make a subject access request ("SAR") at any time to find out more about the information which the Charity holds about them.

- SARs should be made in writing, addressed to The Data Protection Officer.
- A SAR should be clearly identifiable as a SAR.
- SARs must make it clear whether it is the data subject themselves that is making the request or whether it is a person acting on his or her behalf. In either case, proof of identity must be provided. If the SAR is made on another's behalf, the individual making the request must provide clear evidence of their authorised capacity to act on behalf of the data subject.

11.2 The Charity currently requires a fee of £10 (the legal maximum) for each SAR, payable by cheque.

11.3 Upon receipt of a SAR the Charity shall have a maximum period of 40 calendar days within which to respond fully, but shall always aim to acknowledge receipt of SARs within 5. The following information will be provided to the data subject:

- Whether or not the Charity holds any personal data on the data subject.
- A description of any personal data held on the data subject.
- Details of what that personal data is used for.
- Details of how to access that personal data and how to keep it up to date.
- Details of any third-party organisations that personal data is passed to.
- Details of any technical terminology or codes.

11.4 Data subjects must make a formal request for information we hold about them. This must be made in writing. Employees who receive a written request should forward it to the Data Protection Compliance Manager immediately.

11.5 When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

a) We will check the caller's identity to make sure that information is only given to a person who is entitled to it.

b) We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.