



DATA PROTECTION POLICY

POLICY & PROCEDURES

Author:	Manager - KPC	Date: 19 Nov 13
Title:	Data Protection Policy	Version: 0.1

Registered Office: Off Pyle Inn Way, Pyle, Bridgend, Mid Glamorgan CF33 6AB
Tel: 01656 745399 or Tel/Fax: 01656 749219
Charity Company No: 1123339 Company No: 6247822
Email: kpcyouth@hotmail.com



DATA PROTECTION

1	<p>At KPC Youth, in accordance with the Data Protection Act (1998), we understand that:</p> <ul style="list-style-type: none">• <u>DATA</u>: relates to information that is recorded and processed on a computer, or recorded in a relevant filing system, by reference to individuals or criteria relating to individuals• <u>PERSONAL DATA</u>: means data relating to a living individual, who can be identified from the data. It also includes opinions about an individual and any indication of intentions in respect of that individual, eg: notes regarding offering a job etc• <u>DATA CONTROLLER</u>: means a person(s) who determine the purposes for which, and the manner in which any personal data are processed	
2	<p>We will ensure that:</p> <ul style="list-style-type: none">• Data is only used for the purposes on which it was obtained, eg: charities commission, funders, CRB, QES etc.• We only give personal data to people who are entitled to receive it• We establish the identity of telephone callers before giving them personal data, and if there is any doubt regarding their identity, ask them to request information in writing• Take every care to ensure that data stored is up to date• Ensure procedures are in place for protecting data securely• Treat any related personal information which we see as Confidential• We will adhere to this policy also when dealing with information relating to others using our premises – eg: PRU pupil information• Information is only kept for the recommended legal retention time, or to meet with funder's requirements, then destroyed appropriately and securely• If information on individuals is to be entered on monitoring systems such as the Families First QES system, we will obtain permission from the individual in the first instance that they are in agreement with this• Personal/confidential work data is not stored on personal devices – eg: mobile phones, tablets etc	



	<p>We will not:</p> <ul style="list-style-type: none"> • Tell other persons (including colleagues) about confidential information we have used or seen unless we have permission to do so 	
3	<p>At KPC we will ensure compliance to meet with the eight data protection principles</p> <ul style="list-style-type: none"> • Fairness & legality – <i>All data will be processed fairly and lawfully. No one should be misled about the purpose for which their data is processed</i> • Permission – <i>Personal data will only be obtained and processed for specified and lawful purposes with permission from the data subject for each use</i> • Accuracy – <i>We will endeavour to keep data as accurate and up to date as possible</i> • Length of Use – <i>We will ensure that personal data is kept for no longer than is necessary for the purpose it is intended for</i> • Access Rights – <i>Data subjects have the right to access their personal data, and to prevent processing that is likely to cause them damage or distress</i> • Security – <i>We will take appropriate measures to ensure against unauthorised processing of personal data/accidental loss or destruction of personal data</i> • Transfer outside the EU – <i>not applicable to our organisation at present</i> • Computer Security – <i>computers safety and security procedures to be followed. Passwords are in place for key computers processing data</i> • Disclosure of Personal Data – <i>Care will be taken that inappropriate disclosure of data is not made, and that particular care will be taken in the use of emails and their contents</i> • Manual Records – <i>all manual records and files containing personal data shall be securely locked when the Manager’s office is unoccupied, and will not be accessible to other employees unless they require the data to carry out their duties</i> • Particular care will be taken over sensitive personal data (eg: relating to racial/ethnic origin, political opinions, religious or similar beliefs, 	



	trade union membership, physical or mental health, sex life, offences or alleged offences and associated proceedings)	