SANJARI
INTERNATIONAL COLLEGE

Data Protection Policy and Procedure

June, 2013

The purpose of this policy is to enable Sanjari International College to:

- Comply with the law in respect of the data it holds about individuals;
- Follow good practice;
- Protect Sanjari International College's staff, students, service users and other individuals
- Protect Sanjari International College from the consequences of a breach of its responsibilities.

Legal Framework

The Data Protection Act 1998 regulates the collection, storage, use and disclosure of information about individuals by organisations. Any organisation that keeps information about individuals must comply with the act. The Act applies to personal data - information about identifiable living individuals that is:

- Held on computer or any other automated system
- Held in a relevant filing system (a paper system such as client records system, or a set of files on service users that is organized alphabetically by the name of the person or some other identifier such as case number)
- Intended to go onto computer or into a relevant filing system

Good practice principles

The Data Protection Act sets out eight enforceable principles of good practice. These principles are that the data must be:

- Fairly and lawfully processed;
- Processed for limited purposes and not in any manner incompatible with those purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept for longer than is necessary;
- Processed in accordance with individuals' rights;
- Secure.

Policy Statement

Sanjari International College needs to collect and use personal data (see paragraph below) about our service users, employees and other individuals, who are referred to in the Act as “data subjects” in order to carry out our business effectively and provide high quality services. We hold information about data subjects for service provision, administrative, personnel management and membership management purposes.

Sensitive personal data

The Act defines "sensitive personal data" as personal data consisting of information as to racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; membership of a trade union; physical or mental health or condition; sexual life; the commission or alleged commission of any offence or any proceedings for any offence committed or alleged to have been committed, including the disposal of such proceedings or the sentence of any court in such proceedings.

The purpose for which we hold sensitive personal data about data subjects is for use solely for equal opportunities monitoring or for the provision of specific services to individuals. This includes but is not limited to: the provision of services to members and service users, assessing suitability and fitness for work, administering sick pay and sick leave, absence control, maternity leave and pay, parental leave, paternity leave and pay, adoption leave and pay, safe environment, complying with our obligations under the Disability Discrimination Act.

Statutory purposes

In addition to the purposes outlined above, we may collect, hold and process data including sensitive personal data if it is necessary to do so for compliance with any statutory duty with which we are required to comply.

Marketing activities

Sanjari International College will also comply with the terms of the Act and with other relevant legislations such as the Privacy and Electronic Communications (EC Directive) Regulations 2003, in relation to its marketing activities. Direct marketing refers not only to selling products and services to individuals, but also includes promotional activities. All individuals, without exception, have the right to prevent or stop their personal information

being used for direct marketing. Sanjari International College will state how personal information will be used and how individuals will be contacted.

Data Protection Procedure

The following procedure is designed to ensure that Sanjari International College has mechanisms in place to ensure the principles of the Data Protection Act 1998 are adhered to. This section provides guidance to all staff, on their obligations in respect of accessing, holding or using personal information during the course of their employment or such as service user information and information relating to other members of staff. It applies to all employees. Those managing others should take particular notice of content, however, since they may have additional responsibilities under the Act.

Sanjari International College will ensure that:

- There is someone with specific responsibility for data protection within the organisation
- All personal information collected will be factual and objective
- All those who manage and handle personal information understand the requirements of the Act and their responsibilities under it
- All those who manage and handle personal information are appropriately trained and supervised to do so
- The methods of handling personal information are regularly audited, reviewed and evaluated

Responsibilities

This policy applies to all staff. The procedure aims to set out the steps by which personal data is collected, the requirements to ensure records are completed appropriately and the requirements for the handling, storage and destruction of records.

1.1 Senior Staff member

Responsible for ensuring that all records are maintained and stored in accordance with the policy and procedure in place and adhered to. Also responsible for destruction of records in accordance with policy and procedure

1.2 Staff

Responsible for compliance with the policy and procedure

2. Staff Responsibilities

2.1 Senior Person

- To ensure that all staff and service users have access to and are aware of this policy
- To ensure that safeguards are in place to protect the interests of the service user

2.2 All staff

To be aware of and adhere to this policy and procedure

The Act requires that all personal information is kept confidential and secure. You must therefore:

- Observe all instructions or directions given to you in respect of confidentiality and security of information;
- Comply with all security obligations under our Computer use and telecommunications Policy;
- Comply with all confidentiality obligations contained within your employment contract;
- Keep workstations locked when away from desks and keep any documentation containing personal information out of sight overnight, not left out on desks;
- Inform the organisation of any changes to your personal details to enable us to comply with the Act and to aid the smooth running of the business;
- Keep all lockable cabinets and drawers in which personal information is stored locked when not in use; and
- Treat any documentation taken out of our offices in the same way as when in the office, ensuring security of information
- Information held must be accurate, relevant and not excessive. If you need to hold or collect personal information you must therefore:
    - Ensure that all documents containing personal information are up to date and held for no longer than is necessary; you should be aware that what

constitutes “no longer than necessary” will vary and takes into consideration the type of information and the purpose to which it is to be put;

- Ensure that all documentation or other materials no longer required containing personal information are disposed of via secure destruction bins / shredders; and
- Ensure that the content of personal information held is objective; the information you hold may be disclosed to the individual concerned.

Staffs need to ensure that only the “authorised processing of information” takes place. In practice this means that:

- Information held and used must be required by you in the course of your employment; you must not access, gather or hold information which you do not genuinely need in order to carry out your role;
- Access to personal information should be refused to individuals both internally and externally (without the consent of the data subject), unless it is clear that these individuals are authorised to access or process such information.

Except in certain limited circumstances, it is a criminal offence to obtain or disclose personal data or the information contained in personal data or to procure the disclosure of the information contained in personal data to another person without the consent of the person responsible for our compliance with the Act.

This means that:

- You may be committing a criminal offence if you do not process data in an authorised manner, whether you do so deliberately or because you have not taken sufficient care;
- You must comply with the terms of this Policy and with any further instructions or directions given to you;
- If you have any doubts or queries concerning your access to, or use of, personal data in the course of your employment you should seek guidance from your Manager or any relevant Compliance Officer.

2.3 Sanjari International College Staff training

Staff responsible for the management of personal data must have had training in the provisions of the Data Protection Act 1998.

All staff working with personal data need to be reminded that it is a disciplinary offence to disclose confidential information to unauthorised individuals.

3. Audit Plan

The Manager/ senior person will monitor adherence of the policy and report findings to the CEO.

4. Third Parties

We do not normally have the need to provide information we retain on any of our staffs or service users to organisations or individuals outside Sanjari International College other than to Social Services and other related statutory bodies during the course of client reviews and to any company which Sanjari International College employs to undertake its administration processes. When we are asked to participate in client reviews, for referral purposes, or for any other reason we intend to pass information to another agency, we will always inform the client or staff member of the information we intend to reveal and seek their agreement.

Data may also be disclosed to others at a data subject's own request.

7. Photographs

We will request consent before taking any photographs of individuals and will let them know how any photographs will be used.

8. Electronic communications

We monitor electronic communications by employees and service users including to websites, to ensure that these systems are used in accordance with our internet policies.

9. Employee obligations

In the course of our business, we collect and process personal information, including that relating to service users, employees, contacts, and suppliers to which you may have access

in the course of your employment. It is our policy to ensure compliance by our employees with the Act.

We reserve the right to implement the Problem Resolution Policy against anyone who fails to comply with the procedures set out in this policy and procedure.

10. References

Providing a reference involves the disclosure of personal data of the individual who is the subject of the reference. So that we can ensure we protect our employees' data no references (whether to prospective employers or other institutions) should be given on behalf of the organisation without prior authorisation from the senior person.

This Policy does not prevent any employee giving a reference in a personal capacity but employees should make clear that such references are personal and not on behalf of the organisation and, if the reference is given on paper, that neither the organisation's name, address nor logo appear on the paper. It is our policy to provide copies of references given by us to the individual who is the subject of the reference if they request a copy.

11. Marketing

We will inform individuals how and by whom their information will be used. This will include telling them that information may be shared with other organisations with similar aims and objectives. When we collect information from people and are in direct contact with them such as in a phone call or via our website, we will provide an immediate opportunity for them to opt out of further contact and to let us know how they would like to be contacted.

We will not make unsolicited **phone calls** to any organisation or individual who has told us they do not want our calls, or to any number on the Telephone Preference Service list.

We will not send unsolicited marketing by **electronic mail** to individuals without first getting their permission.

We will not send unsolicited **fax** marketing to anyone who has a number on the Fax Preference Service, or who has told us they object.

In all our marketing we will identify who we are and provide contact details so that the recipient can contact us.

If an individual decides they no longer want to receive marketing, we will deal with their request promptly.