Document Control

Policy Title	Confidentiality Policy
Policy Number	069
Owner	Human Resources Manager
Contributors	Human Resources Manager
Version	1.0
Date of Production	01 October 2014
Review date	01 October 2016
Post holder responsible for review	Human Resources Manager
Primary Circulation List	Shared Drive
Web address	N/A
Restrictions	N/A

Version Control

Version Number	Owner	Description	Circulation
1.0	Human Resources Manager	Review	SMT

1.0 INTRODUCTION

Employees are required at all times to maintain absolute confidentiality in respect of matters which come to their knowledge in the course of their work. All employees of SHS must appreciate that they are the custodians of private client, employee and Company related information. All written matters in connection with clients, employees and general Company issues are highly confidential and must not be communicated to anyone outside the organisation.
Employees are also required and expected to maintain this standard of confidentiality when they leave employment with this organisation.

This policy relates to client records, staff records, computerised systems and general company information. This document outlines the way in which information is to be used appropriately to ensure confidentiality for individuals in line with our legal responsibilities and good practice.

2.0 SCOPE:

All employees and volunteers and students and agency of Sunbeam House Services

3.0 POLICY:

SECURITY OF CLIENT FILES AND RECORDS
Contents of client files are confidential and, in some cases, the details of family backgrounds can be highly sensitive. Matters, which are confidential regarding clients, must never be discussed outside the workplace or divulged to any unauthorised third party. Disclosure of information to others should be on a "need to know" basis only.

Quite apart from embarrassment to the individuals concerned, disclosure of confidential information could lead to legal action.

Clients or their guardians have a right of access to information held in client records which is recorded by SHS, but do not have the right to access information in the client file recorded by professionals outside SHS. Permission for access in the latter case must be sought privately from this source (refer to Freedom of Information Act 1997 - 2003). Decisions regarding the release of any information will only be made after formal written application to S.H.S.

STORAGE OF CLIENT FILES:
Files, which may include diaries, record books, programme notes or other information, must be kept in a lockable cabinet. Keys should be kept by the Client Services Manager or the nominated employee on duty.

The cabinet should be secured and kept locked and should be accessed by permission of the Client Services Manager. Permission should be requested for each and every

inspection of the file from the service User and notified to the reporting Manager. Client files held on each location are the responsibility of the Client Services Manager.

ACCESS TO CLIENT CONFIDENTIAL INFORMATION

Access to confidential information will only be granted to those employees who are involved in the direct support of a client. For any other employees this will only be with the permission of the Client Services Manager or appropriate Senior Services Manager. Access to information is discretionary, if there is any doubt about this, the matter should be referred to the Senior Services Managers.

Permission to handle files should not be given to anyone who is not directly involved with the support of the service user. Where exceptions are required to be made to this general rule, reference should be made to the Managing Director for special permission. The reporting Manager may wish to give limited access to only parts of the file to certain people, i.e. students.

DISTRIBUTION OF CLIENT FILES

Under no circumstances should files be allowed to leave the location in which they are normally stored except under special circumstances as directed by the reporting manager and then signed for by the person taking the file.

Files should be clearly marked for what they are, and they should have no loose sheets, all sheets should be stapled in or properly bound as appropriate. The filing cabinet should be organised so that the absence of a file is recorded and immediately identifiable. The loss of a file should be reported immediately to the appropriate Manager.

CLIENT ASSESSMENTS AND REVIEWS

Every user of SHS services must have their needs thoroughly assessed by the Admissions Committee before services are provided. This necessarily involves the staffs who carry out an assessment or handle assessment material sent to SHS from other external agencies in learning a considerable amount about an individual. It is the duty of such employees to retain, record and pass to the allocated employees only the information which is relevant to the person's future support needs. A similar obligation applies to staff involved in regular reviews or reassessment of Client needs or in making any changes in the service provided.

HANDLING OF SERVICE USER INFORMATION BY EMPLOYEES

Employees assisting a service user have access both to the information passed to them when they start to work with that service user and to knowledge which accumulates in the course of supporting the service user. They have a duty of confidentiality:

a. To treat all personal information with respect and in the best interests of the service user to whom it relates

b. To share with their Reporting manager, when appropriate, information given to them in confidence
c. To share confidential information when appropriate with colleagues with whom they are sharing the task of supporting the service user
d. To pass and receive confidential information to and from colleagues on occasions when they have to be replaced because of sickness, holidays or other reasons, in a responsible and respectful manner
e. Only to pass confidential information to other social and healthcare agencies with the agreement of the service user, with the permission of the Client Services Manager, or in emergencies when it is clear that it is in the interests of the service user or is urgently required for the protection of the service user or another person
f. To refer to confidential information in training or group supervision sessions with respect and caution and preferably in ways which conceal the identity of the service user to which it relates
g. Never to gossip about a service user or to pass information to any other individual other than for professional reasons.
h. Employees, volunteers, students and agency staff should respect Client privacy and should never identity a service user by their name. Client identify and information should only be shared with relevant individuals on a needs to know basis

COPYING

Only in exceptional circumstances will client files be copied. Where copies of these files are required, this must be done by the reporting Manager or nominated person by the reporting manager, and if possible the copying machine should be used by that person themselves. Care should be taken that spoiled copies are properly destroyed and that no extra copies are left floating or visible to third parties.

EMPLOYEE RECORDS

This policy also applies to all records and information held by the company concerning staff. The Human Resources Manager is responsible for all staff records.

EMPLOYEE ACCESS REQUESTS

If an employee wishes to request access to their own HR personnel file, The employee should send a letter or email to the Managing Director to request to view your HR personnel File.

GENERAL INFORMATION

No information relating to clients, staff or Company must be removed from any of SHS premises without permission from the Reporting Manager.

All company documentation must be marked “confidential”, including outgoing mail and emails, which contains personal client information, employee or company information.

When employees are discussing service user issues, ensure this is done in a private confidential place.

PUBLICATIONS, REQUESTS FOR INFORMATION AND INTERVIEWS

Publication of any matters relating to the affairs of SHS must have the prior approval of the Managing Director.

Requests for information or interviews from media services - radio, TV or press, should be forwarded to the Senior Services Manager. The giving of interviews, making of statements, or relaying of any other information connected with the services provided by this organisation must not be undertaken without the prior approval of the Managing Director.

Public statements by all employees of SHS may be taken as reflecting SHS policy. Therefore any information must only be issued through authorised spokespersons. Leaking of any information to any source, including making it available to colleagues not connected to a particular location, is not permitted.

MEMBERS OF THE PUBLIC

All employees have a duty to deal with members of the public and clients with the utmost courtesy and impartiality. When dealing with the public and in the performance of their duty, employees should at all times observe the requirements of courtesy, consideration and promptness and should at all times give their name when communicating by telephone.

MOBILE WORKING

It is each individual employees responsibility to adhere to the policy when mobile working or working from home and ensure that information is not easily accessible to others that are not employed by SHS. This is true of mobile devices and documents that are in an employee's possession. Employees should not leave confidential or sensitive documents in their cars or at locations where they can be easily read or stolen.

ICT SYSTEMS

In compliance with the Data Protection Act, 1988 & 2003, SHS has taken measures to guard against unauthorised access to computer based personal data and against its alteration, disclosure or destruction.
The Information and Communication Technology (ICT) Manager is responsible for defining the level of access considered appropriate for individual employees, and issuing passwords.

EMPLOYEE PASSWORD PROTECTION

Employees issued with passwords must ensure that their password is not made available for use by unauthorised persons, or disclosed for use by others unless specifically instructed to do so by the ICT Manager. Employees must not seek access to systems for reasons other than the performance of their official duties. Employees will treat as

confidential all information to which they have access via the computer systems. Employees have a responsibility to bring to the attention of the ICT Manager any known breach of this policy. Employees must at all times comply with all other ICT policies.

PERSONAL BREACH OF DATA SECURITY

1. The Data Protection Acts 1988 and 2003 impose obligations on data controllers [1] to process personal data entrusted to them in a manner that respects the rights of data subjects to have their data processed fairly (Section 2(1)). Data controllers are under a specific obligation to take appropriate measures to protect the security of such data (Section 2(1)(d)).

2. The data breach management policy addresses situations where personal data has been put at risk of unauthorised disclosure, loss, destruction or alteration. Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the employee must follow the data breach management policy.

3. All incidents in which personal data has been put at risk should be reported as per the Data breach management policy.