Integrated Neurological Services

CONFIDENTIALITY POLICY

INTRODUCTION

This policy has been drawn up to meet the needs of Integrated Neurological Services (INS), its staff, volunteers, service users and Board members.

The policy exists to ensure that basic standards are adhered to by all those parties mentioned above and which are incorporated and maintained as part of normal working practices.

This Policy is designed to cover all aspects of confidentiality pertaining to the work of INS and its associates. The Board, staff and volunteers will be made aware of this policy when first joining the organisation and will be asked to sign an undertaking indicating that they have read and understood the policy and will abide by it.

Where reference is made to INS premises this includes:-

- 82 Hampton Road, Twickenham, TW2 5QS
- Any other premises from which INS may operate.

1. PERSONAL DATA

1.1 Each staff member/volunteer working for INS will have a personnel file containing confidential information. Personnel records should be kept in a locked cabinet. Access to these files will be by their supervisor, in the case of volunteers, the line manager, the Office Administrator and by the Chief Executive Officer (or their nominees) and where appropriate, Trustees in the case of staff members. Should information contained in these files come to light by means of accident or any other way, to anyone other than the appropriate supervisor or employee/volunteer themselves, then such information should not be divulged to a colleague, volunteer or other third party within or outside the organisation.

1.2 Each individual staff member/volunteer will have the choice as to whether they wish their home telephone number, personal mobile number, address, or any other personal details, to be divulged to any other person either inside or outside the organisation, other than to be kept as a record for personnel purposes within their personnel file. If a staff member/volunteer has not specified whether or not they would wish such information to be given to a third party, then such information should not be given without prior consultation with the employee/volunteer concerned.

1.3 Personal data held for each employee will include sensitive data relating to sickness records, health records, ethnic origin and trade union / non union membership, and is subject to the provisions of the Data Protection Act.

1.4 Personal details pertaining to Board members may also be kept on record within the organisation. Specifically, a list of Board members must be available for public inspection. This list would include individuals' names and addresses, but not telephone numbers. Any other personal information, other than that mentioned, pertaining to Board members shall not be divulged either within or outside the organisation, other than with that individual's consent and as advised by the Chief Executive Officer.

2. SERVICE USERS

2.1 INS offers a number of confidential services to users and it is therefore implicit that such confidentiality is respected. Therefore, clients' details should not be disclosed or discussed with anyone outside the organisation in such a manner that it is possible to identify the client, unless the client agrees to such information being passed on to a third party. An enquirer's approach is to the organisation rather than to an individual employee or volunteer. Therefore if the needs of a particular client are best served by discussion with another staff member/volunteer, then such disclosure does not breach the policy. If, however, a client specifically requests that information is not divulged to a third party of any kind, then this wish should normally be respected.

2.2 The situation often arises when an enquiry is made on behalf of someone else (third party), e.g. by a relative; friend or neighbour, and in these circumstances it is allowed to give general advice or information to the enquirer. However, should a specific request be made for help or assistance that would necessitate INS referring the potential client to a third party, or INS visiting that person, then a request must be made by the person themselves for such assistance either verbally or in writing. If the individual concerned is not in a fit state mentally or physically to give such permission, it should be sought by their carer, next of kin or advocate, as may be appropriate in the circumstances. If a staff member/volunteer is in any doubt whatsoever about the validity of the third party enquiry, they should consult with the Chief Executive Officer, or member of staff with authority to deputise.

2.3 Records and files relating to service users are available to staff and volunteers who have undergone selection/training and who have signed the statement on confidentiality. Care must be taken at all times to ensure that all records/files are handled with discretion and are not left around on desks or in public view. The same principles should be applied with confidential information in memos, letters, briefing papers and minutes of meetings. When client records are not in use they should be kept in locked cabinets.

2.4 The same principles of confidentiality shall apply to all clients, whether they are being dealt with in person, by correspondence or by telephone.

2.5 If it is necessary for staff/volunteers to remove confidential information

regarding clients from any premises, e.g. on home visits or to attend meetings, due care and attention must be exercised to ensure that such material is kept safely in their possession at all times. Particular care should be taken with personal diaries which may contain details of service users such as names and addresses. No such material/information should be left unattended. Electronic diaries, personal computers and phones should be password protected if they hold any client information.

2.6 When emailing several people the same message the message should be sent "blind", so email addresses cannot be seen by other recipients. When entering names on the email, click on "cc". In the dialogue box that opens enter names into "**bcc**" line rather than "to" or "cc" lines.

3. ORGANISATIONAL INFORMATION

3.1 Staff, volunteers and Board Members may receive confidential or sensitive information relating to INS or other organisations. The same standards of confidentiality should be adhered to as is the case with clients information been dealt with at INS. Such information should only be divulged to a colleague or third party within the organisation, and never to anyone outside without consultation with the Chief Executive Officer or the Chairman.

3.2 Confidential information pertaining to any aspect of INS's work or policies should not normally be sent by fax, however, if it is necessary to do so, the first page should clearly indicate that the material is confidential and who should receive it. Prior arrangements should be made with the recipient to ensure that confidentiality is not breached. The same principle applies to email.

3.3 Any confidential or sensitive matters pertaining to any aspect of work of INS, its staff, volunteers or Board members should not in any circumstances be discussed with any third party outside the organisation, without prior discussion with the Chief Officer. Nor should such information be discussed with a third party within the organisation without prior consultation with the person it concerns or the Chief Executive Officer, whichever would be the most appropriate, depending on the nature of the information (eg personal or organisational).

3.4 INS, its staff or Board members will abide by any information sharing protocols requested by statutory organisations provided they are no less stringent than the requirements of this policy.

4. BOARD MEETINGS

4.1 Board Members shall be expected to comply with the same standards of confidentiality specified in this policy at all general and special meetings of the organisation. Specifically, in respect of any confidential agenda items, Board members will be expected to adhere to the policy and guard against any breaches either intentional or unintentional.

4.2 Any staff members, volunteers or staff representatives attending any such meetings must also comply with the standards of confidentiality as set out in

this policy and guard against any breaches either intentional or unintentional.

4.3 Any minutes produced as a result of such meetings shall not be divulged to a third party outside the organisation, without prior consultation with the Chief Executive Officer. Any minutes that exist of any confidential agenda items, particularly pertaining to named individuals, should not be disclosed to any person or third party excluded from discussion of such agenda items, either inside or outside the organisation, unless specifically authorised by the Chief Executive Officer or Chairperson of any such meetings, as may be appropriate.

5. DATA PROTECTION ACT (1998)

5.1 The Data Protection Act regulates when and how an individual's personal data may be obtained, held, used, disclosed and generally processed. It applies to computer processing of personal data and certain paper based file and records.

5.2 To comply with the law, information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. To do this INS will comply with the Data Protection Principles set out in the Data Protection Act. In summary, these state that personal data will be:

- Processed fairly and lawfully and will not be processed unless certain conditions are met
- Obtained for specified and lawful purposes and not further processed in a manner which is incompatible with that purpose
- Adequate, relevant and not excessive
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Processed in accordance with the data subject's rights
- Protected by appropriate security
- Not transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

5.3 INS is registered under the Data Protection Act. If there are any queries that arise relating to the Act, advice should be sought from the Chief Executive Officer. Serious breaches in confidentiality will be reported to the Information Commissioner's Office in accordance with their guidelines.

6. THE CALDICOTT REVIEW

6.1 The Caldicott review was carried out for the NHS in 1997 and this identified a set of good practice principles and standards which provided a framework for the management of confidential information for all NHS organisations.

6.2 With the increase in joint working with health and other agencies, there is now a requirement that all Councils Social Services' departments and partners ork towards the same framework.

6.3 All staff are expected to be aware of the following six Caldicott principles and apply these when considering how personal information is being used, held or shared:

- Justify the purpose for holding personally identifiable information
- Do not use personally identifiable information unless necessary
- Use only the minimum necessary
- Access should be on a strict need to know basis
- Everyone with access should be aware of their responsibilities
- Understand and comply with the law

7. Breach of confidentiality

7.1 Confidentiality may be broken in the following circumstances:

- Where the person from whom the information was obtained and, if different, the person to whom it relates, consents
- Where the information is in the form of a summary or collection to information so framed that it is impossible to ascertain from it information relating to any particular person.
- Where the information is already available to the public from other sources
- When there is a serious risk of harm to the individual
- To safeguard others.
- To prevent a serious criminal act, especially where others may be endangered.

7.2 With the exception of the first two points above, any proposed disclosure of personal information should, if possible, be discussed with the Chief Executive prior to disclosure.

7.3 Nothing in this policy shall prevent you from disclosing information which you are entitled to disclose under the Public Interest Disclosure Act 1998 ("whistleblowing") , provided always that the disclosure is made in accordance with the provision of the Act.

8 Termination of employment and data

8.1 Upon termination of employment all data and information relating to the INS must be returned immediately. The restriction of confidentiality of data and information will continue to apply after the termination of your employment but will cease to apply to any information which may come into the public domain through disclosure by the INS.

Integrated Neurological Services

CONFIDENTIALITY POLICY

Declaration of Intent

I, the undersigned, have read Integrated Neurological Services Confidentiality Policy. I understand its context and intent and agree to abide by it at all times

Name: ……

Position: .....
(e.g. staff member, volunteer, Board member)

Signature: ……

Date: ……