1. Introduction

Options aims to make a difference to the lives of the people we support through the provision of high quality care, education and therapeutic services. Options recognises the importance of protecting the confidentiality and right to privacy of all service users and staff members. This policy sets out the Group’s policy relating to confidentiality, privacy and data protection legislation concerning all service users and staff. It provides a framework of guidance within which all local procedures must be set.

- It is the responsibility of line managers to ensure that staff members are aware of and understand this policy.
- All staff are individually accountable for observing the confidentiality and data protection principles described in this policy regarding all information obtained at work.
PART 1 – CONFIDENTIALITY & PRIVACY

2. Principles of Confidentiality

- Options operate a strict policy with regard to confidential information.

- Staff members must not at any time during their employment or afterwards, to the detriment or prejudice of the Company including service users, customers or suppliers, use or divulge to any third party, except in the proper course of their duties during employment, any confidential information identifying or relating to the Company including service users, details of which are not in the public domain, or such confidential information relating to the business which have come to their knowledge during employment.

- All staff members must sign the Staff Confidentiality Agreement at the start of their employment. See template CPD1.

- Each service holds records of a personal nature for service users, staff and the company. All records, whether medical, financial or social will be safeguarded to protect the confidentiality of each service user and staff member.

- Any breach of confidentiality is a breach of trust, whether the trust of the service user or the Company, and as such, the Company will regard any breach of confidentiality as a serious disciplinary offence and it will be referred for action under the Company’s Disciplinary policy. Depending on the seriousness of the offence, it may amount to potential gross misconduct and could render the staff member liable to summary dismissal.

- Information obtained by staff as a result of their work, whether personal or company information, must be respected as confidential and not disclosed to any third party, other than as described below, without the consent of:
  - the individual to whom the information refers,
  - and/or a person entitled to act on their behalf,
  - and/or the Head of Service/Function

- Staff discussing confidential information for a legitimate purpose must ensure that the circumstances in which they are having their discussion does not lead to a breach of confidentiality (e.g. discussions in front of other service users/visitors, in corridors, car parks, pubs, restaurants etc.).

- Malicious gossip regarding colleagues or any gossip relating to a service user is never permissible, is unprofessional and considered a breach of trust.

- In the case of company information, all requests should be referred to the Head of Service/Function, who will refer any cases of doubt to Central Office for a decision.

- All cases where disclosure is required by Law must be communicated to and authorised by the Head of Service/Function and advice sought from the HR department if applicable.

Privacy of Service Users

- Respect for the privacy of service users is vital to the development of their sense of self-esteem, individuality and personal safety. The following principles are expected as a basic minimum:
  - Lockable storage for possessions
  - A single room
  - For staff/other service users to knock and await an answer before entering their room
  - For staff or other service users not to show visitors their room unless they agree
  - To be able to receive visitors in private
  - To be able to make telephone calls in an area where they will not be overheard
  - To send and receive mail without hindrance (unless explicitly restricted in their Plan).
• To be able to access an appropriate area for religious observance
• To have a guaranteed period of leisure time each day which they can spend alone

• Photographs of service users in services should only be taken with the informed consent of the individual concerned or, if they are unable to give consent, following discussion with parents and the placing authority. See Marketing - Privacy & Electronic Communications Policy for further details.

3. Limits of Confidentiality

• In the event that a service user does not give their permission to disclose any information provided, information must not be disclosed or repeated to anyone else.

• In the event that a service user discloses information in confidence and the information may compromise the health and safety or well being of themselves or others, this information should be disclosed to a senior manager with the knowledge of the service user.

• Any confidential information disclosed in a staff member’s supervision must remain confidential between the supervisee and supervisor unless there is a disclosure or practice which may need to be referred to a senior manager.

• Confidential information and records containing this information may be freely discussed by those responsible for the care and education of the service user, including the Head of Service. Disclosure to other services within the company will only be permitted:
  • On referral or transfer of a service user;
  • In the event of a complaint or serious untoward occurrence;
  • In the event of an inquiry;
  • In other circumstances, at the request of the service user.

• Staff must not disclose information other than as specified in this policy, except where disclosure is required by the Order of a Court or is necessary in the “public interest”. In public interest cases, action will be taken by the Head of Service.

4. Discussing Confidential Information with Significant Others

• Staff wishing to discuss confidential information with a relative or friend of the service user should ensure that they take the following precautions first:
  • Consult the personal plan to clarify the relevant agreements;
  • Consult the service user themselves to ascertain their views;
  • Consult the key worker. Wherever possible, any discussion with family members should be undertaken by the key worker.

• In the case of any doubt, consultation may be made with the placing authority, via the senior member of staff in charge.

• Staff should remember that, in certain cases, there are compelling reasons why discussion of confidential information with family or friends would be significantly detrimental to the interests of the service user. In cases of doubt, do not divulge; seek advice from a senior manager.

5. Sending Confidential Information

• Detailed steps to secure the confidentiality of information disclosed in telephone conversations, letters, email etc. will be subject to local procedures for each service.

• Do not send confidential information by fax, unless the sender is convinced that the intended recipient will receive the fax in person at the time of transmission.
• Confidential information sent by post should be clearly labelled “Private and Confidential” and for the attention of the addressee only. It is a matter of local discretion whether certain information should be sent by recorded delivery.

• Any discussions involving confidential information over the telephone should be treated with extreme caution. Local procedures should ensure that all callers are adequately identified before information is passed on. If necessary ring back the caller to verify that they are who they claim. Be especially cautious if given a mobile number. Check that callers or those called are in circumstances where they can conduct a conversation involving confidential information, without risk of breaching confidentiality.

PART 2 – DATA PROTECTION AND ACCESS TO RECORDS

6. Data Protection Principles

• The Data Protection Act relates to personal information held on both staff and service users. Information protected by the Act includes not only personal data held on computer but also certain manual records containing personal data, for example staff member personnel files that form part of a structured filing system.

• It works in two ways:
  1. To give individuals certain rights, whilst requiring those who record and use personal information on computer and in manual files to be open about that use.
  2. To follow sound and proper practices.

• There are eight data protection principles that are central to the Act. The Company and all its staff members must comply with these principles at all times in their information-handling practices. In brief, the principles say that personal data must be:

  1. Processed fairly and lawfully and must not be processed unless certain conditions are met in relation to personal data and additional conditions are met in relation to sensitive personal data. The conditions are either that the staff member has given consent to the processing, or the processing is necessary for the various purposes set out in the Act. Sensitive personal data may only be processed with the explicit consent of the staff member and consists of information relating to:
     • Race or ethnic origin.
     • Political opinions and trade union membership.
     • Religious or other beliefs.
     • Physical or mental health condition.
     • Sexual life.
     • Criminal offences, both committed and alleged.

  2. Obtained only for one or more specified and lawful purposes, and not processed in a manner incompatible with those purposes.

  3. Adequate, relevant and not excessive. The Company will review personnel files on a regular basis to ensure they do not contain a backlog of out-of-date information and to check there is a sound business reason requiring information to continue to be held.

  4. Accurate and kept up-to-date. If staff member’s personal information changes, for example they change address or they get married and change their surname, they must inform their line manager as soon as practicable so that the Company’s records can be updated. The Company cannot be held responsible for any errors unless staff members have notified the Company of the relevant change.
5. Not kept for longer than is necessary. The Company will keep personnel files for no longer than six years after termination of employment. Different categories of data will be retained for different time periods, depending on legal, operational and financial requirements. Any data that the Company decides it does not need to hold for a period of time will be destroyed after approximately one year. Data relating to unsuccessful job applicants will only be retained for a period of six months.

6. Processed in accordance with the rights of employees under the Act.

7. Secure. Technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, data. Personnel files are confidential and are stored in locked filing cabinets. Only authorised staff members are permitted to have access to these files. Files must not be removed from their normal place of storage without good reason. Personal data stored on diskettes or other removable media must be kept in locked filing cabinets. Personal data held on computers must be stored confidentially by means of password protection, encryption or coding and again only authorised staff members are permitted to have access to that data. The Company has network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed.

8. Not transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the processing of personal data.

- **Registration:** Each Options Company is registered under the Data Protection Act for the storage of personal information concerning staff and service users. Any new applications concerning the use of personal information must be discussed with Central Office and agreed in advance to ensure that the terms of registration are not breached.

- **Content:** All information held on staff or service users, whether or not on an administrative system, should be obtained lawfully and fairly. Items of hearsay or personal comment must not be recorded in the individual record. Any opinions or conclusions should be as the natural outcome of professional observation and assessment and should have been discussed with the service user or staff member in advance. Only items which are relevant and verifiable should be included. Speculation is not permitted. Items intended to be retained in the records for a fixed period, such as staff disciplinary warnings, must be removed following expiry. Changes to circumstances, plans, or personal details must be promptly recorded and dated.

### Rights to Access Records

#### 7.1 Staff

- The Company holds personal data about staff members and staff member’s consent to the Company processing personal data is a condition of their employment. Therefore, by a staff member agreeing to their contract of employment, they also agree to their personal data being held and processed. The Company also holds limited sensitive personal data about its staff members and, by signing their contract of employment, they give their explicit consent to the Company’s holding and processing that data, for example sickness absence records, health needs and equal opportunities monitoring data.

- Under the provisions of the Act, staff members have the right on request to receive a copy of the personal data that the Company holds about them, including their personnel file to the extent that it forms part of a relevant filing system, and to demand that any inaccurate data be corrected or removed. Staff members have the right on request:
  - To be told by the Company whether and for what purpose personal data about them is being processed.
  - To be given a description of the personal data and the recipients to whom it may be disclosed.
• To have communicated in an intelligible form the personal data concerned, and any information available as to the source of the personal data.
• To be informed of the logic involved in computerised decision-making.

• In general, there are no areas of their record that should be forbidden to staff. The only exception may be the content of references received prior to employment, in which case the referee should be informed and permission sought. In these circumstances, please seek advice from the HR department.

• Upon request, the Company will provide staff members with the document requested, time to view their personnel file or a written statement regarding the personal data held about them. A written statement will state all the types of personal data the Company holds and processes about staff members and the reasons for which the data is processed.

• If staff members wish to access a copy of any personal data being held about them, they must make a written request for this and the Company reserves the right to charge you a fee of up to £10 per request. This request must be responded to as soon as possible and no later than 40 days after the staff member has made their request.

Rights to access records procedure

• To make a request, staff members must contact the Administration department. Discretion on the charge may be provided depending on the information requested.

• The right to access is not immediate and may only be granted upon receipt of a written request and payment of a £10 administration fee depending on the information requested.

• Prior to providing the staff member with their personnel file, the manager responsible for the file should check that all items within it:
  − Relate to the staff member concerned and do not contain confidential information about others
  − Are relevant and appropriate to be kept in the staff member’s personnel file. Just because a staff member is mentioned in correspondence does not mean that copies of that correspondence should be placed in their personnel file

• Staff may only view their file in the presence of the Administration Manager at an agreed time.

• Staff may not remove any items from the file and should indicate sheets that they wish to copy.

• Staff should indicate to the manager present any sheet of paper with information that they wish to have corrected, removed or to challenge. These sheets will be copied at the companies expense and each signed and marked to show the selected items by the staff member and the Administration Manager present.

• The manager will produce a covering sheet listing all the sheets under consideration and summarising the issues for each.

• Copies will be sent to the staff member and Head of Service, who will consider the representation and respond to the staff member with their decision and justifications.

• Only at this point may any items be removed from the personal file, in line with the Head of Service/Function’s decision.

• Access to information should not be withheld and the Law requires disclosure within 40 days, though in practice, managers should strive to ensure as near immediate access as possible.
7.2 Service Users

- Correction of information in respect of service users should be undertaken in conjunction with the placing authority and any changes should be notified to all those with a need to know.

- Information can only be withheld from a service user if disclosure could be against their best interests or constitute a serious breach of confidentiality. Any case should be referred to the Head of Service and discussed with the placing authority.

- Details of the information withheld, with reasons, must be recorded and signed off in the individual’s records by the manager.

- Family members may only be permitted access to a service user’s records following discussion and agreement with the service user and under staff supervision. The keyworker would normally deal with all requests. Any cases of difficulty, especially where the relative has only restricted access to the service user, should be referred to the Head of Service and discussed with the placing authority.

- Authorised representatives of Placing Authorities have a legal right to access information held on service users for whom they are responsible. As a matter of good practice, this access should be granted in the company of the keyworker or Manager, who have detailed knowledge of the service user involved. Any strong objection by the service user should be discussed with the placing authority and family and a strategy agreed.

- Statutory Inspection Agencies are entitled to access to individual records, for the purposes of inspection only.

- All other requests must be placed in writing, stating the status of the individual making the request, their reasons and details of the purposes for which they will put the information to use. The Head of Service will institute full discussion with the service user, relatives, placing authority and possibly the police. No request will be approved until the consent of these parties has been obtained in writing, with details of any conditions. Access will only be granted under strict supervision by a senior manager.
APPENDIX 1

LIST OF SUPPORTING TEMPLATE FORMS AND LETTERS

- **CP1** Staff Confidentiality Agreement

The above list of template forms and letters, in Word format, can be found on the Options Resources Portal at [http://www.optionsgroup.co.uk/resources/resources_downloadable_res.php](http://www.optionsgroup.co.uk/resources/resources_downloadable_res.php).

Please refer to the latest monthly update email for current log-on details for the Portal. Local Administration departments can assist where required.