Confidentiality policy

POLICY STATEMENT

A.S.S is a partnership of voluntary, statutory and community bodies. Professionals who work for statutory bodies must first and foremost adhere to their individual codes of conduct. Regarding confidentiality A.S.S staff must adhere to A.S.S policies and procedures.

Our intent is that this is not just a policy but the basis of how we practice, a value base and an ethos for all A.S.S staff, not just inside working hours, but to include expectations of staff outside working hours.

A.S.S is committed to promoting best practices of confidentiality regarding personal, professional, organisational and user's information. Whilst we aim to respect an individual's right to confidentiality and information, we recognise that guarantees of absolute confidentiality cannot be assured if:

1. a child, young person or vulnerable adult's safety is a risk;

2. there are suspicions of an arrestable or criminal offence having occurred to the detriment of the group;

3. there is a concern that there has been unprofessional conduct by anyone working for the group.

This policy aims to ensure the confidentiality of all verbal and written information collated and disseminated through A.S.S services. Confidential information about A.S.S families or staff must not be disclosed to any unauthorised person.

This policy relates to recorded information, whether written or held on computer. However, it should be remembered that spoken information can also be confidential, and as such is subject to the same consideration and restrictions.

Any outside agencies with which A.S.S have contact should be aware of our confidentiality policy and that not all information held can be passed on.

They should also be aware of our open access policy and should be asked to label confidential information as such, and explain what restrictions apply.

Any breach of confidence will result in the disciplinary procedure being invoked.

Procedures for the recording and storage of confidential information should ensure confidentiality is maintained.

PROCEDURES

This policy statement and procedures are applicable to the A.S.S Partnership Board, staff and volunteers.

A.S.S registered with the Data Protection Agency on ??? 2003 and will continue to register annually thereafter.

DATA PROTECTION ACT 1998 - INFORMATION FOR USERS/STAFF/VOLUNTEERS

1. The Data Protection Act 1998 imposes obligations on “data controllers”, persons who either alone or jointly with others, direct how and why data is processed.

2. "Personal" data is information, in electronic or written form, concerning a living person who is identifiable from that data, or from other data which is in the possession of the data controller. There is a sub-category of personal data known as sensitive personal data, namely that which relates to an individual’s political opinions, racial or ethnic origins, mental or physical health, religious persuasion, trade union affiliation or criminal record. The obligation’s imposed on data controllers and data processors are more onerous for sensitive personal data than other personal data.

3. Processing is so widely defined that it may be assumed it covers everything done with it - obtaining, recording, organising, using, disclosing or holding it.

4. A data processor is someone, other than an employee of the data controller who processes data on behalf of and at the direction of the data controller e.g. pay roll bureau.

THE EIGHT PRINCIPLES OF DATA PROTECTION

There are 8 principles with which data controllers must comply:

i. Personal data must be processed fairly and lawfully. To this end, Sure Start will always take steps to ensure, as far as possible, that family members know the data controller and the purpose for which the data is to be used. It is up to individual family members as to whether they provide sensitive personal data. Only where it is necessary for the legitimate interests of Sure Start will it process information for the actual or complied consent of the individual. It is the responsibility of all A.S.S staff who process personal data to ensure they do so fairly and lawfully.

ii. Personal data must only be obtained and processed in line with the purposes stated in the notification. It is the responsibility of A.S.S staff to satisfy themselves their processing is for a notified purpose.

iii. Data must be adequate, relevant and not excessive in relation to purposes for which it is processed. It is similarly the responsibility of the A.S.S staff member to ensure the adequacy and relevance of the data, and that it is not excessive.

iv. Data must be accurate. This principle is similar to “principle 3” above. Staff must ensure that information is properly documented initially, and (insofar as this is practicable) that it is kept up to date.

v. Data must not be kept longer than necessary. The principle again follows on from “principle 3” above. If the purpose for which the data was obtained is no longer relevant, the data must be erased. For data to be stored consent must be provided by family members. The only exception to this is where the data is retained for research of statistical purposes only (see later).

vi. Data must be processed in accordance with the rights of the data subject, as detailed in section two above. Access must never be refused without the written authority of the data controller. A request for data to be rectified or erased must similarly never be refused without the express written authority of the data controller.

vii. Appropriate technical and organisational measures must be taken to protect against unauthorised or unlawful processing of data or of its loss or destruction.

viii. Data must not be transferred outside the EEC unless it is to a country that has an adequate level of protection for the rights and freedom of data subjects in relation to the processing of the data.

Individual rights

From 24th October 2001, any person upon which data is held by an agency will have a number of rights under the Data Protection Act 1998. These include:

- the right to access their personal information
- the right to have a copy of information
- the right to correct any inaccuracies in that information

Please note that A.S.S may not always be able to allow a member of staff or a service user access to information where disclosure would provided information about another individual who could be identified from the information or as the source of the information.

If any person wants to access personal data, please contact the Project Co-ordinator of A.S.S project. We charge an administration fee of £10 for access to such information, and access can be arranged by appointment only and will occur within 40 days of a written request.

Personal Information

What information should be treated as confidential?

- Any information about a family’s personal affairs is confidential, as is any

- information about family members. For example children's files, creche records, monitoring information etc.
- Personal information in relation to staff is also covered by this policy. For example, information in relation to recruitment and selection of staff, interview records, supervision notes etc.
- Information in relation to A.S.S project. For example minutes of Partnership Board meetings, Agendas, Business plans etc.

Who has a right to access information?

Anybody has right of access to information where data is held on that person, unless it is for the performance of a contract, it is in the interest of the public or there is legal obligation to hold the data.

Staff information

Staff will be aware that personal information will be collected from them when they first register or apply for employment. This information is held on file.

In relation to short listing for staff, confidentiality rules are agreed by the panel prior to the interviews taking place.

For individuals employed through the project, application forms are held on file, for up to one year, with the other applicants who applied for the post. Personal details are held on our computer system, which is password protected, and monitoring slips are held separately.

When staff leave A.S.S project their staff records will be kept for a period of 3 years.

For those applicants who are Reserve Candidates data will be held for 6 months and the data will then be shredded. However, at the end of this 6 month period if the organisation wishes to extend this waiting list for a further 6 months the Reserve Candidate will be contacted and asked to confirm in writing if they wish to remain on the waiting list for a further 6 month period.

For those candidates who were unsuccessful at interview data will be shredded after one year.

The monitoring of the movements of the actions of staff by way of CCTV, or the random checking of e-mails, website use or telephones is covered by the Data Protection Act 1998. The Human Rights Act 1998, the Regulations Investigatory Powers Act 2000 and the Telecommunications Regulations 2000.

Issues arising from e-mail and website monitoring are covered in the IT and Laptop Policy which is made available to all staff as part of their induction.

Personal data covers opinions as well as facts, therefore an individual may request access to employment references received by, and given by, A.S.S. Any giving of a reference has to be in accordance with the first data protection principle - that of

being fairly and lawfully processed. Therefore an employee must have given prior consent. It is important to remember that information regarding sickness or misconduct is sensitive for which express consent is required in order for it to be retained or disclosed. In relation to references, an employee is not legally entitled to have access to a reference given by A.S.S, however they can demand it from the recipient of the reference, providing the identity of the reference is excised.

FAMILY INFORMATION

During an initial visit users are provided with an explanation informing them that we adhere to the Data Protection Act and requesting that they sign a consent form that will enable us to store their information in our premises. All staff and volunteers are aware that their records are kept with personal details and that an open access policy applies. However, in exceptional circumstances, the project reserves the right to withhold information if it deems that this disclosure would be inappropriate.

All users' details are held on a computerised system which is password protected for processing and monitoring purposes.

Sensitive personal data (racial, ethnic, religious or political origin) will only be held with consent or for the purposes of monitoring equal opportunity or legal rights.

Filing cabinets (with keys) are provided to all staff to store all confidential material. Cabinets should be locked when the offices are unattended and no confidential information should be left on desks. Our clear desk policy requires that no files are left on the desk overnight.

Information held on computers may only be accessed by authorised users.

Access to data will be restricted to authorised users and adequate security measures, including computer passwords, will be in force.

Staff will be informed of any changes in legislation or policies.

If staff or volunteers breach confidentiality, this will be dealt with via the disciplinary or grievance procedure being implemented.

Sharing of information

A.S.S staff will in the course of their duties have access to, and be entrusted with, information relating to children and their families.

Parents/carers are entitled to expect that any information about family circumstances, children's health, development and behaviour shared with or observed by staff or volunteers will be treated in the strictest confidence.

Sensitive information about individual children, given by parents/carers to a A.S.S member of staff will not be shared unless there is a need to know or a pressing need and the parent/carer has granted permission for the information to be shared except under exceptional circumstances.

There may be an occasion when in order to protect an individual, there will be those in the group who are told relevant information on a 'need to know' or 'pressing need' basis. These disclosures will take place at a specified time and agreed meeting place. Staff who are passed confidential material are bound by the A.S.S Confidentiality policy and Standards of conduct.

In some exceptional circumstances the right to access information is restricted:

- Access to records may be denied if it is considered the disclosure of this information would be likely to disturb or cause serious harm to the mental health of the family member or someone else.
- If the records include confidential information about a third party, and where that person refuses their permission.
- If the records include information obtained in confidence from a third party and where that person refuses their permission.

Under no circumstances should a family member have access to the files of other families or staff members.

Information may not be given to a third party except where an individual has a legal right to act on behalf of another person.

However, consideration of confidentiality should not override the right of children to be protected from harm. In instances where there is an allegation or suspicion of abuse, confidentiality needs to be broken in order to protect the child. It is important to ensure that only those who need to know are given the relevant information in order to protect the rights of the victim and the alleged perpetrator (Cross reference: Child Protection Policy).

The data controller is to be informed of all applications for data access. Prior to the information being provided the staff member must familiarise themselves with the family making the request and ensure the file or computer information contains the relevant information requested.

Staff conducting a formal investigation, have access to any information relevant to the pursuance of a case and s/he will be the judge of relevancy.

If a criminal act is believed to have been committed, the PSNI have powers to remove or copy any information that could be used as evidence.

Any staff member who has access to records should be instructed on this policy and appropriate procedures. This should form part of their induction.
Implications of open access record keeping

Implications of open access record keeping

Records should be thorough and accurate so as to fulfil their intended use. The possibility of access by family members or others should not alter the content of records or be used as an excuse for incomplete record keeping.

Where the comments of third parties are registered in family records, these individuals may request that their contributions remain confidential. The quality of information sharing should not be diminished by fear of open access.

Procedures involved in recording and sharing information

Information should be recorded, stored, read and discussed in ways that preserve confidentiality.

Recording and reading should take place in a private location.

Storage of documents should be in an office, and all documents should be locked away when not in use. Documents should remain on A.S.S property. If for some reason they are to be removed, permission of the Project Co-ordinator must be obtained in advance.

The loss of any document relating to a family should be reported to the Project Co-ordinator immediately. Any third party known to have been named in the document should be contacted and the loss explained.

Computer records of confidential information should have a security system preventing access by any unauthorised person. The security of computerised information containing personal details of identifiable living people is a statutory requirement under the Data Protection Act, 1984.

Managers may wish to keep separate files for particularly sensitive information.

When a child is too old to access A.S.S programmes their records will be kept for a period of 3 years. However, if there is a child protection concern or a safe handling issue records will be kept until the child's 21st birthday. Concerns of a criminal nature, such as sexual abuse or pornography may be kept indefinitely.

Responsibility of administrative staff

Reviewing the contents of all files (manual and electronic) to ensure any personal data held complies with the eight principles.

Reviewing application forms, employment contracts and other documents to ensure that all information systems comply with the standards of fair practice and good procedure contained in the data protection principles.

Informing data subjects of the identity of the Data Controller, the nature of the data held, the purpose for which it is held and the likely recipient of the data

The changes heralded by the Police Act 1997, the Protection of Vulnerable Children

Act 1999, the Care Standards Act 2000 (Including the Protection of Vulnerable Adults provisions) and the Disclosure procedure operated by the Criminal Records Bureau and Codes of Practice relating thereto, place a heavy emphasis on the principles underlying the Data Protection Act and the Human Rights Act with regard to disclosures of criminal offences. Separate policies exist in this regard, but it is emphasised that any improper disclosure of such intensely sensitive personal information would necessarily be treated as a serious disciplinary matter.

All staff who maintain manual or electronic records containing such data must review it regularly, and ensure not only that explicit consent has been obtained to retain it, but that it is necessary to keep it. If it is, then a process must be put in place to ensure that, from time to time, its accuracy is confirmed.

Training Sessions

Prior to training sessions taking place a contract is drawn up between staff, volunteers or users outlining the rules in relation to confidentiality.

Receiving confidential information

All post is opened and recorded by the administrator. Staff are reminded to inform organisations who may be sending confidential information to ensure they inscribe on the envelope "Private and Confidential".

Telephone calls of a private nature should be taken in private by staff and volunteers. There are additional telephones in A.S.S premises to provide staff with this facility in that eventuality.

Those staff who receive confidential minutes of meetings must agree to adhere to our confidentiality procedures. All committee business should be treated with confidentiality.

When a member of staff or volunteer leaves the project it is their responsibility to hand in all documentation relating to families.

Consent for the taking and storage of photographs

Written consent of the individual, or that of the parent/carer of a child under 18 years of age, who will appear in the photograph, must be obtained for the use in Sure Start material and storage, before a photograph is taken, used and /or stored.

Photographs will be stored for a period of 3 years and then destroyed. Permission to keep photographs for longer than three years must be sought annually.

Permission to use the photographs for use in publications which are in general circulation must be obtained before each and every instance.

CROSS REFERENCE TO OTHER POLICIES

Discipline and Grievance; Standards of Conduct; Child and Vulnerable Adult Protection; Recruitment and Selection; IT and Communication;

For inclusion in handbooks

Introduction

The Data Protection Act 1998 means that we have to have clear systems for all data handling in A.S.S. The policy attached outlines what we need to do to ensure A.S.S complies with the law. The act contains eight principles (see below) which need to inform how we use and handle data.

The rules of good information handling - the eight principles

Anyone processing personal data must comply with the eight, enforceable principles of good practice. These state that data must be:

1. fairly and lawfully processed
2. processed for limited purposes and not in any manner compatible with those purposes
3. adequate, relevant and not excessive
4. accurate
5. not kept for longer than is necessary
6. processed in line with the data subject's rights
7. secure
8. not transferred to countries without adequate protection

Data controllers and managers

What is a data controller?

The Data Controller is the legal entity that decides why information is processed and is responsible for how it is processed. This is A.S.S, as an organisation.

A.S.SPB co-ordinates the data protection system manually.

What is a Data Co-ordinator?

A.S.S has a Data Co-ordinator who is responsible for introducing and maintaining a data protection system in the project and liasing with the Data Controller's representative.

A.S.S Co-ordinator is the person responsible for ensuring that the eight principles apply within the A.S.S project.

What is a Data Manager?

Data Managers are personally responsible for ensuring that the data is processed according to the law.

Data Protection

A.S.S maintains a central database of information on all its employees in order to allow us to communicate effectively, monitor the success of our equal opportunities policy, manage levels of sickness absence and ensure the safety of our service users. In particular the database contains the following information:

1. **Personal data on an employee's gender, ethnic origins, disability and religion**.
   This is used to produce reports that allow us to monitor the effectiveness of our equal opportunities policy

2. **Dates and length of any absence and the reasons for that absence.**
   This is used to monitor levels of absence across the organisation and to produce individual absence reports. These may be used to discuss your attendance record, to take action as a result of this record and to stop salary in the event of you exceeding your right to A.S.S sick pay.

3. **Records of attendance at training events and individual skills and qualifications.**
   These will be used to monitor skills across the organisation and in your workplace. They may also be used in helping us to manage and/or demonstrate your performance or capability at work.

4. **Records relating to any grievances, disciplinary issues or performance concerns including instances when no formal action has been taken.**
   In addition to a database, manual records will be kept. These manual records will contain reference to the allegations that have been made, minutes of meetings and any accompanying written evidence and a note of any decisions made

The above will only be passed to a third party if this is required in order to:

1. Complete an application to provide a service

2. Conduct a defence against allegations that may be made against us in an employment tribunal or similar court of law

It is a requirement of your employment that you give your explicit consent to the above data being recorded, processed and kept by A.S.S.

You have the right to view any data held on you.