Introduction to Data Protection and Confidentiality Policy

Deafconnect needs to keep information about its Staff, Trustees, Volunteers and Clients to allow it to run efficiently and effectively for the benefit of those we serve.

Deafconnect recognises that a guarantee of confidentiality is an important factor in determining the level of trust and security its service users hold in the organisation.

The purpose of this policy is to establish a clear and agreed understanding of what Data Protection and Confidentiality means within Deafconnect, to ensure that we operate within the legal framework and consistently across the organisation, and that service users know what they can expect from the organisation.

Scope of Policy

This Policy has been developed in conjunction with Deafconnect Staff, Trustees and Volunteers and applies to everyone acting on behalf of Deafconnect. This continues to apply after their service or involvement with Deafconnect has ended.

This policy applies to all employees transferring to Deafconnect through TUPE arrangements. TUPE employees will be subject to the procedures outlined within this document with exception to retaining their previous contractual terms and conditions as set out within their written statement of terms and conditions of employment (with exception to where measures have been agreed).

TUPE refers to the "Transfer of Undertakings (Protection of Employment) Regulations 2006" as amended by the "Collective Redundancies and Transfer of Undertakings (Protection of Employment) (Amendment) Regulations 2014". The TUPE rules apply to organisations of all sizes and protect employees' rights when the organisation or service they work for transfers to a new employer.

Data Protection

To comply with the law, information must be:

- Collected and used fairly
- Stored safely
- Not disclosed to any other person unlawfully

To do this, the eight Data Protection Principles set out in the Data Protection Act 1998 must be followed and these are summarised below.

i. Personal data (information about identifiable, living individuals held on computer or in a manual filing system) must be obtained and processed fairly and lawfully

ii. Data can only be collected and used for specified purposes (People have a right to refuse giving us data; purpose of collecting data should be explained at time of collection)
iii. Data must be adequate, relevant & not excessive (Data must be fit for purpose but can be "accurate enough").
iv. Personal Data must be accurate and up to date.
v. Personal Data must not be held any longer than necessary
vi. Data Subjects' rights must be respected. People are entitled to see data relevant to themselves People have the right to opt out of direct marketing.
vii. Data must be kept safe from unauthorised access, accidental loss or damage includes gossiping and overhearing,
viii. Special rules apply to transfers abroad (including publication over the Internet)

Deafconnect staff, Trustees and volunteers who process or use any personal information in the course of their duties must ensure that these principles are followed at all times.

All information given to Deafconnect must remain at Deafconnect once Staff, Trustees and volunteers have left Deafconnect. No information given to Deafconnect may be used by ex staff/ volunteers/trustees once they cease their association with Deafconnect.

In order to ensure that this happens, Deafconnect has drawn up the following to relate to:-

- Service users
- Volunteers, Staff and Trustees

Important Note: "The Data Controller"

Deafconnect as a body is the Data Controller under the Act, and the Deafconnect Board of Trustees is ultimately responsible for the policies' implementation. However, Deafconnect has designated Joanna Steer who will deal with any day-to-day matters arising from the implementation and interpretation of Data Protection policy.

Personal Data relating to service users

Purposes

Deafconnect obtains contact details (names, addresses, phone numbers) as well as other personal details including gender, ethnicity, deafness and disability from service users. This data is obtained, stored and processed to assist volunteers and staff in the efficient running of the service requested by the client; to respond to statutory and contractual requirements and to provide statistics to assist in targeting and development of services. Personal details supplied by service users may be

used to send Deafconnect's marketing material or newsletter where consent has not been withheld; however, service users should be given the opportunity to opt out of this.

Informing the consent and gaining consent

Personal data from new service users is collected by telephone, email, text or face to face interview and recorded by appropriate staff. During this initial contact, the client is informed of the details of the service and given an explanation of how their personal data will be used (for example: to ensure service users receive service that meets their specific requirements and to enable Deafconnect monitor services in line with funding agreements). Confirmation that this explanation has been given will be recorded on the database (referral) entry form.

Third party referrals - When a referral is made via a third party (for example: a relative or friend), if the client is present a similar explanation will be given to them as detailed above. If they are not present, this explanation will be given the first time the client is met.

Sharing service users' personal data – A client's personal data will not be passed on to anyone outside Deafconnect (for example: doctor, social worker) without explicit consent from the client unless there is a legal duty of disclosure under other legislation e.g. safeguarding or professional practice requires this. In the event of consent being withheld, the procedures in Deafconnect's confidentiality will apply.

Access

Only staff and volunteers will normally have access to service users' personal data and this will be on a need to know basis. All staff and volunteers are made aware of Deafconnect Confidentiality Policy and their obligation not to disclose personal data to anyone who is not authorised to have it.

Request for records - Service users will be supplied with a copy of any of their personal data held by Deafconnect if a written request is made. A charge will be made and will be based on material used, a reasonable contribution to overheads and time taken to provide the information. The maximum charge allowed by statute (currently £10) will be made. Service users will be informed of the charge at the time the request is made and will be provided with the copy within 10 working days unless otherwise notified.

Accuracy and Longevity

Staff and volunteers will take reasonable steps to keep Personal Data up to date and accurate and ensure corrections are made to the database in a timely manner. Personal Data will be stored for one year after the client's death or until the client is 100 and has not received a service for one year. Once the entry is closed, anonymous data may be retained for statistical and/or research purposes.

Storage

Personal data stored in paper filing systems are to be kept in a locked filing cabinet when not in use. Access to computer records containing service users' personal data is controlled by password and a systematic back up routine is in place. Where a volunteer/staff member/trustee is also a service user further levels of security will be put in place in line with Deafconnect's confidentiality policy.

Use of photographs

Where practicable, Deafconnect will seek consent of service users before displaying photographs in which they appear. If this is not possible (for example: a large group photo) Deafconnect will remove any photograph if a client or a relative/friend of the client makes a complaint. This policy also applies to photographs published on the Internet.

Personal Data relating to Staff, Volunteers and Trustees

Purposes

Deafconnect obtains contact details (names, addresses, phone numbers), application forms, references and in some cases other details such as driving documents from Staff, Volunteers and Trustees. This data is stored and processed for the following purposes:

a) Assessing the suitability of an applicant for a specified role
b) To keep track of availability, training course attendance record and other necessary details with respect to volunteering opportunities;
c) To distribute relevant Deafconnect material (for example: the newsletter, board papers).
d) Payroll, work planning, absence monitoring, pensions

Staff, Trustees and Volunteers are responsible for notifying any changes to personal details

Staff, Trustee and Volunteer changes including banking arrangement should be notified direct to the CEO.

Access

Only the contact details and details of staff/volunteer/trustees availability are made accessible to other staff/volunteers of Deafconnect. The rest of the information supplied on application is kept in a locked filing cabinet or other secure medium and is not accessed during the day-to-day running of Deafconnect.

Contact details of volunteers/staff members/trustees will not be passed on to anyone outside Deafconnect (for example, a client) without explicit consent.

Request for records

Volunteers/staff members/trustees will be supplied with a copy of all their personal data held by Deafconnect if a written request is made. A charge may be made and this will be notified at the outset of the inquiry (current maximum defined by statute is £10) and where possible the copy will be issued with 10 working days unless otherwise notified. Where the volunteers/staff members/trustee is also a service user, Deafconnect's confidentiality policy will apply. Access to third party material such as references, medical information etc. may not be possible.

Accuracy and Longevity

Reasonable steps will be taken to keep Personal Data up to date and accurate and make corrections in a timely fashion. Personal Data will be stored for as long as the volunteer/staff member is working for Deafconnect and for six years after they have left. Once this period has elapsed, all Personal Data held by Deafconnect on the volunteer/staff member will be reviewed and, other than basic contact details, destroyed unless there is good reason not to do so. Good reasons include statute and potential and/or current litigation. Data on trustees as members of the company will be kept for 20 years. Data relating to unsuccessful employment or volunteering applications will be destroyed 12 months after the date of last interview.

Storage

Personal data stored in paper filing systems are kept in a locked filing cabinet when not in use. Contact details of volunteers/staff members/trustees kept as computer records are only accessible by members of staff and volunteer office workers.

Use of photographs

Where practicable, Deafconnect will seek consent of staff before displaying photographs in which they appear. If this is not possible (for example: a large group photo) Deafconnect will remove any photograph if a member of staff or a relative/friend of the member of staff makes a complaint. This policy also applies to photographs published on the Internet.

Compliance

In compliance with the Data Protection Act, Deafconnect is registered with the Information Commissioner in order to process data. Our registration number is available upon request.

CONFIDENTIALITY

Confidentiality is important for several reasons. One of the most important elements of confidentiality is that it helps to build and develop trust. It potentially allows for the free flow of information between the client and worker, Staff member and Management, acknowledging that a person's personal life and all the issues and problems that they have belong to them.

Respect for client confidentiality and staff personal information is of high priority for Deafconnect and we ensure that we comply with legislation that governs disclosure of information and appropriate worker behaviour.

Responsibilities and Arrangements for Confidentiality

The Board of Trustees

The Board of Trustees as the employer has overall and final responsibility for ensuring that Deafconnect meets its legal responsibilities regarding confidentiality in relation to criminal record checks, the Data Protection Act and any current or subsequent human rights legislation, which guarantees a right of privacy. The Board of Trustees will review the operation of this confidentiality policy annually.

The Chief Executive

The Chief Executive Officer (CEO) has overall responsibility for ensuring that the confidentiality policy is put into practice. In particular the CEO will ensure that:

Core training encompasses Confidentiality and Data Protection Awareness training and is available to all staff and volunteers.

General Principles

Information belongs to the person or agency entrusting it to a member of staff or volunteer of Deafconnect. Once received by Deafconnect, information held (including Deafconnect information) may not be used for any purpose other than that for which it was given; nor may it be passed on to any person or agency outside Deafconnect without the express permission of the giver.

There may be circumstances where consent is not given and it is thought necessary to breach this condition. How to do this is dealt with below.

Operational Practice

Deafconnect keeps extensive records using paper and electronic files; where necessary, personal details of Deafconnect staff and users of a Deafconnect service are recorded in these systems. Each staff member and individual user of Deafconnect services has the right to see any information that Deafconnect keeps on them in paper or computer files and to change that information where it is inaccurate. Confidential information that has been provided by a third party may be removed from a file prior to its examination. Deafconnect will maintain an appropriate

level of security, in accordance with its Data Protection and Social Media policy. Paper files will be kept in locked storage units and electronic files will be password protected; employees should only access confidential information for work that is covered by their job description. The use of information for reports, monitoring and funding applications will scrupulously avoid any specific detail about service users that might lead to their identification, unless they have given their permission for it to be so used. The data provided by Deafconnect should not include information that could easily lead to the identification of service users.

Occasions when the policy may be broken

Deafconnect acknowledges that, on rare occasions, it may be necessary to break the basic rules of confidentiality. These may broadly be defined as situations where the safety, rights and liberties of other people or the person giving information may be seriously at risk. Also, legal reports may have to be made regardless of the consent of a service user. In such cases, staff should discuss the matter with the CEO. Decisions that are made, and the reasons for them, must be properly recorded on the Breach of Confidentiality Policy monitoring form – Appendix B, this is then stored in the individuals file. When confidential information is divulged without consent (e.g. child or vulnerable adult protection, terrorism, money laundering, drug dealing and immigration issues) except where it might result in more harm to other people, the individual concerned should be informed and an explanation of the action given by copy of the Confidentiality Policy monitoring form.

Children and Young People

Confidentiality is particularly important when dealing with children and young people. However in some cases parents and guardians have to be informed of issues which arise during the course of work. Confidentiality may also be broken if a child or young person discloses information which indicates that he/she has a safe guarding issue. Staff should then refer to the procedure set out in the Deafconnect's Safeguarding policies. If a member of staff or volunteer has any cause for concern about an issue which a child has disclosed or discussed then, in the first instance, the worker should speak to the CEO as soon as possible. The incident and all actions should be meticulously recorded.

Dealing with information

This refers to all information that:-

1. is or has been acquired by the employee/volunteer/trustee during, or in the course of their employment/volunteering, or has otherwise been acquired by the employee/volunteer/trustee in confidence,

2. relates particularly to Deafconnect, or that of other persons or bodies with whom Deafconnect have dealings of any sort, and

3. has not been made public by, or with our authority

Information shall be confidential, and (save in the course of the business or as required by law) an Employee/volunteer/trustee shall not at any time, whether before or after the termination of their employment/volunteering, disclose such information to any person without written consent or use this information to benefit another organisation.

Employee/volunteer/trustee is to exercise reasonable care to keep safe all documentary or other material containing confidential information, and shall at the time of termination of your employment/volunteering with Deafconnect, or at any other time upon demand, return to the CEO any such material in their possession.

Sharing information within Deafconnect

In order to give the best possible service to Deafconnect's service users, it is desirable to share information with other colleagues in Deafconnect. This is on a need to know basis and at the discretion of the CEO. Similarly, it is important that in supervision meetings, staff and volunteers should feel able to talk freely about their experiences.

Information given to staff members or volunteers acting on behalf of Deafconnect is, in these circumstances, considered to be given to Deafconnect as an agency, rather than to the individual staff member or volunteer. However, it should be absolutely clear to all attending such meetings that they are bound by the Deafconnect's rules of confidentiality and that confidential matters must not be discussed outside Deafconnect. Casual or social discussion about service users that is conducted amongst Deafconnect staff whether inside or outside Deafconnect premises is strictly prohibited and any breach of this requirement would be dealt with as part of the Performance Management process and may lead to disciplinary proceedings.

Access to files

Whilst everyone has right of access to their own files under the Data Protection Act, parents do not have a right to see their children's files unless they are acting on behalf of the child (where a child is unable to act for themselves). Children have the right of access once they are capable of exercising their rights independently and this is considered to be around the 12. This means that applications from children around that age will have to be assessed on a case by case basis to establish whether they are capable of fully understanding the implications of their request.

Where anyone seeks to exercise rights on behalf of another person (adult or child) they may do so provided they are properly authorised and acting in the interests of that person. Authorisation may be via court or established legal rights; however personal knowledge of the applicant may be acceptable. Where their record identifies other individuals, a decision will have to be taken whether to remove them from the record, obtain consent or breach confidentiality. In this case those affected should be informed by way of the Confidentiality Policy monitoring form.

Members of the Board of Trustees

Members of Deafconnect's Board of Trustees include individuals from various backgrounds, some of whom are there in a formal capacity on behalf of other agencies, some of which have statutory duties. Such representatives should normally regard information that they learn as members of a Trustee of Deafconnect as confidential to themselves and to the Board. If, however, as a result of their membership of the Board, they become aware of information that they feel they cannot ignore as a member of a statutory or other body, they should bring this to the attention of the Board so that the statutory or other implications can be formally acknowledged.

Social Media

The term Social Media refers to a number of websites and internet media resources which enable users to share information, opinions and social exchanges. They are normally free to use, are unregulated except by the users themselves, and can be used or looked at by anyone with internet access, anywhere in the world. Examples of social media are blogs, social networking sites (e.g. Facebook and Twitter), podcasts, message boards and chat rooms.

Deafconnect recognises that employees will use these media outside work, and they can be usefully used within work to make business contacts, exchange ideas and views about products and issues, and improve customer service.

Because of the global nature of the media and their potential, some rules need to be devised to ensure the media are used safely and effectively, and these are set out below:

a) During work hours you may only login to the backend of social media streams and make posts on behalf of the Deafconnect if approved by either the CEO or Data Controller(s) of Deafconnect.

b) You may not share any information which is commercially sensitive, private or copyrighted.

c) You must comply with any other guidance we give from time to time concerning use of social media.

d) Be wary of any potential issues concerning information exchanged, such as defamation, breach of privacy and copyright, and comply with the law at all times.

e) You must not identify or refer to any clients, ex-clients or prospects.

f) Be yourself and do not use separate identities or pseudonyms online. If you are on a business related site such as a professional body or business forum, and you think it is appropriate, you may identify yourself with your job title and give the name of your employer. However, you are not speaking on Deafconnect's behalf and if necessary you should state that any views expressed are your own.

g) Use common sense. Apply your judgment and exercise discretion. Respect your audience as you cannot know who is reading your posts. Do not make any derogatory personal comments or offensive remarks. Be mindful that anything you publish is instantly available worldwide and for a long time in the future. It cannot be retracted and you are personally responsible for it.

h) Protect your own privacy and do not disclose any personal information.

i) On your personal social media pages do not identify yourself as connected with Deafconnect.

Review

This policy has been reviewed in consultation with staff and trustees and will continue to be reviewed annually by the CEO.

Approval

This section denotes review and approval dates of this policy document.

Action	Name	Date
Updated	Claire Gogerty	5/01/16
Reviewed by CEO	Joanna Steer	14.03.17
Approved by the Trustees		01.06.17

APPENDIX A

Deafconnect Data Protection Policy

Information for Volunteers, Staff and Trustees

PLEASE READ CAREFULLY

During the course of your duties with Deafconnect, you will be dealing with information such as names/addresses/phone numbers of service users and volunteers, as well as other personal information relating to service users. You may also be told or overhear other sensitive information while working for Deafconnect. The Data Protection Act 1998 gives specific guidance on how this information should be dealt with. In short, to comply with the law, personal information must be collected and used fairly, stored safely and only disclosed to another person in line with the data protection principals detailed above. Normally, Deafconnect would not disclose a person's data without their express consent. Any breach of this requirement would be dealt with as part of the performance review process.

To help you meet the terms of the Data Protection Act while working for Deafconnect, the following guidelines have been drawn up. Please read them carefully and ask Joanna Steer if you are in any doubt about any of them.

1) Sharing service users' personal information

Personal information can include details such as addresses, phone numbers, gender and deafness, professional notes and information from families, friends and other interested parties. Such information may be shared between volunteers and staff at Deafconnect where the nature of the job requires it, but should not be given to anyone outside Deafconnect without explicit consent from the client (but see confidentiality policy). If such a situation arises, please ask Joanna Steer before sharing the information.

Special note on phone numbers – It is the policy of Deafconnect to never give out Staff or Volunteer's personal telephone numbers or mobiles to clients.

2) New Service users

All requests from new service users for any service offered by Deafconnect should be referred to the appropriate member of staff. If that member of the staff is not available, please take a name and contact number only and pass the message on. This is particularly important when dealing with a third party (for example: relative, friend, social worker) as Deafconnect should not collect information about a person who has not given permission to use his/her details.

3) Unlawful Disclosure of personal information

Under the Data Protection Act 1998 you are committing a criminal offence if you disclose personal information 'knowingly or recklessly' to anyone you are not supposed to. As Deafconnect is a small office and clients visit us in the office, please

seek to ensure that conversations are as private as possible, and be aware that conversations containing personal or sensitive information may be overheard or viewed by people who should not have access to it.

4) Use of files, books and card boxes

In order to prevent unauthorised access and accidental loss or damage to personal information held on paper, please take good care of any files, books and card boxes you use while on duty, and ensure that they are stored securely at all times. Files containing personal data should not be removed from the premises without the express permission of CEO. The same requirement applies to personal data held in electronic format (memory sticks, CDs, lap top computers).

5) Disposal of scrap paper

Be aware that names/addresses/phone numbers and details of an enquiry written on scrap paper are also considered to be confidential. If it is not possible to shred the paper, please tear it up prior to disposal. Confidential waste should always be shredded.

6) Your own Personal Information

You may be interested to know that under the Data Protection Act 1998 you are entitled to access any personal information held on you, including that held by Deafconnect. If you want to see this information, please talk to your line Manager who can make the necessary arrangements with HR.

7) Home working

Home working is permissible provided the appropriate technical and organisational safeguards are in place. Please refer to Deafconnect's Home Working Policy.

Members of the Board of Trustees and its sub-committees

Members of Deafconnect's Board of Trustees include individuals from various backgrounds, some of whom are there is a formal capacity on behalf of other agencies, some of which have statutory duties. Such representatives should normally regard information that they learn as members of a Board of Deafconnect as confidential to themselves and to the board. If, however, as a result of their membership of the board they become aware of information that they cannot ignore as a member of a statutory or other body, they should bring this to the attention of the Board so that the statutory or other implications can be formally acknowledged.

Read and understood by Employee, Trustee or volunteer (delete as applicable)

Signed by _____ **Date** _____

APPENDIX B

Breach of Confidentiality Policy Monitoring Form

Name of Deafconnect Employee that is divulging information : _____ Date: _____
Name of Client _____ Was authorisation given by client to divulge information? Yes ☐ No ☐
Circumstances concerning Breach of Confidentiality
Discussed and agreed with CEO date
Has the client been informed that information has been divulged? Yes ☐ No ☐ Outcome of situation:-
Signed Employee: _____ Date: _____ Signed CEO: _____ Date: _____

Copy to be kept by CEO
Copy to be kept on service users file (if applicable)