WiSE
Wetherby in Support of the Elderly

Policy: Confidentiality, Data Protection and Disclosure

Version:	Version 2
Ratified by:	Board of Trustees
Date ratified:	
Author/Originator of title	PERS/C Challoner/M Dobson
Date issued:	February 2017
Review date:	February 2018
Target audience:	**Volunteers, Employees and Trustees of WiSE**

Introduction

WiSE recognises the right to privacy of the individual as a basic human right. We accept that personal details about an individual belong to that individual. Accordingly, we undertake to respect the confidentiality of information.

Purpose

This policy is a statement of our policy and procedure with regard to, Confidentiality, Data Protection and Disclosure of Information

Responsibilities:

- **Employees**
- **Operations Manager**
- **Board of Trustees**

The policy has 4 sections:

General principles

1. General Principles
    - 1.1 Personal information relating to staff
    - 1.2 Subject access requests
    - 1.3 Staff obligations
    - 1.4 Guidelines on disclosing information to internal and external sources
    - 1.5 Organisational information
2. Personal information relating to service users
    - 2.1 Recording and accessing data
    - 2.2 Sharing information
    - 2.3 Collecting and safeguarding information
    - 2.4 Subject access requests
3. Exceptions
4. Confidentiality statement

1. General principles

Personal data is defined as ‘information about a living individual who is identifiable by that information, or who could be identified by the information combined with other data’. It includes names, addresses, identifying descriptions and information relating to individuals such as bank details or personal attributes.

Confidential information is defined as verbal or written information which is not meant for public or general knowledge, or information which is regarded as personal by clients, members, trustees, staff or volunteers. It includes expressed opinion about a person or intentions regarding a person.

This policy relates to the protection of the privacy of staff, volunteers, job applicants, trustees, members, service users and any other person about whom WiSE holds personal information of a formal or an informal nature.

Confidentiality is based upon a reasoned concern for the interests of the person to whose personal information WiSE has access. Respecting confidentiality means that information may be disclosed only with consent and when necessary, and that consultation and discussion remains within those boundaries. This protects the integrity of both WiSE and of individuals.

Where there is uncertainty about issues around confidentiality, advice should be sought from line managers and, where appropriate, trade unions.

Failure to observe this policy or misuse of personal data is a disciplinary offence and may even constitute a criminal offence. Please refer especially to the section titled ‘Staff obligations’.

Data Protection Act 1998

WiSE takes seriously its obligations under the Data Protection Act 1998. We are registered with the Information Commissioner. Responsibility lies with the Operations Manager and should be reported to Trustees in Ops. Manager report to Trustees. Our registration, which is renewed annually, allows us to collect, store and use certain personal information following strict guidelines. These guidelines define the purposes for which we hold

information: in our case, this is information for the purposes of staff administration, [membership administration, fundraising and realising our charitable objectives]. Within these groups, the guidelines define the data subjects (i.e. the individuals about whom that information is held), the classes of data (i.e. what kind of information is held) and the data recipients (i.e. who has access to it).

In particular, the Data Protection Act requires that personal information should be adequate, relevant and not excessive; that it should be stored securely and used only for its intended purposes; and if possible processed only with the consent of the person concerned. WiSE will comply with these requirements and will extend the principles of data protection to apply to all forms of personal information.

1.1 Personal Information relating to staff

WiSE holds information about employees to do with their working life in order to fulfil its responsibilities as an employer. Personal information is also held about Trustees. Much of this information is highly personal and WiSE recognises its duty to safeguard the data by all means possible and to notify staff about what is kept and why, along with information about how the data can be accessed and by whom.

What data?

Information held by WiSE will include:

- Information relating to recruitment and selection such as application forms; shortlisting and interview assessments; references; proof of eligibility to work in the UK; where relevant, unspent criminal records and/or the outcome of Criminal Record Bureau/ Disclosure and Barring investigations.
- Personal details of home address, phone number, next of kin.
- Information necessary for payment of salaries, such as bank details, national insurance number, details of deductions to e.g. the courts or trade unions, expenses claims.
- Information about academic and vocational qualifications and experience.
- Notes of probationary and annual reviews and supervisions.
- Sick notes, and medical assessments, including information relating to disabilities.
- Absence records, including sickness absence, compassionate leave, unauthorised absences.

- Time sheets and holiday sheets.
- Details of grievance and disciplinary proceedings including current warnings (within the timescales allowed by the appropriate policies).
- Reference requests and responses.

'Sensitive' data in particular, such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, or criminal convictions will only be processed if necessary or advantageous to the employment relationship and with the explicit consent of the individual employee. Sick notes, absence records and other health-related information are classed as 'sensitive information' and particular care must be taken to ensure that these are stored securely and that access is limited to staff who need to see them.

Why?

The data kept on staff is primarily in relation to their employment with WiSE. This data will be used for the purpose of administering and managing their employment. Information about trustees is held for registration with the Charity Commission and Companies House and for some funding applications. Personal information about employees and volunteers may also be kept for the purposes of applying for funding, obtaining insurance or responding to requests for information from Government offices, the Charity Commissioners or other reputable bodies. Where possible, sensitive information will not be tied to individuals but will be given in anonymised statistical formats only.

No unrelated data will be kept and any sensitive data (excluding health and criminal records) held by the organisation will be deleted at the request of the individual concerned.

Where?

All personnel data is kept either in locked filing cabinets and /or in password protected computer files. Most personal data is kept in individual personnel files in the Operations Manager's office and these are locked. Other data (e.g. bank details, NI number) is kept by the [payroll officer] on password protected computer files and in a locked filing cabinet. Line managers keep staff files covering supervision sessions plus any job-related information necessary for management.

Some personal information, including names and photographs, may be published in e.g. newsletters, annual reports, publicity leaflets or the organisation's website. This information will not include home or personal contact details. Staff may request that all or any personal information and/or photographs are restricted to internal access and this request should be complied with.

Whom?

Employees and trustees give implied consent to WiSE to hold data as described above and to access and use it as outlined by accepting an offer of employment and agreeing to their Written Statement of Employment Particulars, or in the case of trustees by filling in the Companies House registration form (Charitiy Commission Trustee Eligibility Declaration V6 01/06). Access to staff and trustee data is restricted to management at the appropriate level or to senior administrative staff on a 'need to know' basis. Information may also be disclosed as required by law, contract or on a 'need to know' basis to trustees, auditors, pension providers, funders, insurers, government departments or other relevant parties/individuals. Information will also be given to a transferor as required by law in the event of a transfer of undertaking.

Job applicants are also covered by the Data Protection Act and by this policy. WiSE will design and process application forms and other information relating to applicants in line with the Act. WiSE will only request information which is relevant and not excessive and for the particular purposes of the selection process only. This information will be securely stored and will only be accessed by staff that need to have it for purposes of administration or selection. It will not be kept for longer than necessary for the needs of the organisation, normally no more than twelve months for unsuccessful candidates. Sensitive information relating to health, disability, criminal records and immigration status will only be requested where necessary for the protection of the organisation and/or its service users and will not be disclosed to anyone who does not need to know. Sensitive information relating to gender, age, ethnicity and disability may be requested but will be used for equality and diversity monitoring purposes only. This information will not form part of the selection process and will not be processed or retained in any form which identifies the individual to whom it pertains.

The identity of job applicants should be kept confidential as far as possible and for as long as possible. Where a job offer is made, the names of the successful candidates should not be made public until the appointment has been accepted and confirmed.

Feedback on interview performance should be made without specific reference to other candidates.

How long?

Most information will be retained for as long as a person is employed by WiSE and for a reasonable period of time thereafter, not exceeding 6 years.

Sickness records will be stored securely at all times and will be kept for as long as a person is employed by WiSE and for a reasonable period thereafter, with the aim of destroying or deleting records after 3 years.

Disciplinary proceedings and warnings will be kept for the time stipulated in the policy concerned.

Application forms from unsuccessful applicants to a job will be kept for a reasonable period of time not exceeding six months.

[CRB/DBS documentation will not be retained although a record will be kept of the fact that a satisfactory/unsatisfactory check has been made. This will be kept on file for as long as necessary, or until the next check is carried out.]

I.T.

Personal data held on computers (including files, emails, databases etc) and personal data downloaded from the web are subject to the same control and restrictions as paper-based data. Staff must take particular care when using any personal data in these contexts. In particular, no personal information should be posted on the internet in any circumstances without compelling reasons and the explicit consent of the individual to whom the information relates.

Monitoring of staff activity

Staff should be aware that WiSE may, if they have reason to do so, monitor use of the internet and/or emails. Private emails will never be opened intentionally but staff should be aware of the possibility of accidental access and of the right of managers to question and investigate private use. Deliberate monitoring will only take place where there is good reason to suspect a disciplinary offence or another justified concern. [Please refer to the policy on Private Telephone and Internet Use.]

Performance and quality control monitoring will be overt and for a clear purpose. Covert monitoring will not be permitted.

[CCTV monitoring of staff activity will only take place with the knowledge of staff and for the protection of the organisation and/or its staff and users.]

References

References given by an employer about a person currently working for them are exempt from some aspects of normal data protection rules. This means that an employee has no automatic right of access to a reference written about them by WiSE. However, as a matter of good practice, WiSE will only respond to reference requests that are clearly authorised by the employee concerned.

As a general rule, employment-related references should only be given by the Operations Manager. However, other line managers may provide references for their own staff where appropriate, provided these are checked and authorised prior to sending by the Operations Manager. Personal references should be clearly stated as such and should not be on WiSE headed paper. References must be objective, truthful and justifiable. Telephone references should not be given unless you have been asked to provide one by the person whom the reference concerns, and then you should initiate (or return) the phone call to the person to whom the reference is to be given to confirm identity.

Referees should bear in mind that although there is no automatic right for the subject of the reference to see it before it is sent, they will usually have a right to access any references written about them once they are received by a new/prospective employer.

1.2 Subject Access Requests (SARs)

Staff are entitled to see their own personnel files. To do so, they should arrange a mutually convenient time with their line manager. Access may be denied or limited where it involves disclosing information about or from an identified third party (e.g. a colleague) unless the third party concerned has given consent to the disclosure of that information.

As well as taking action to protect third party confidentiality, WiSE will not respond to subject access requests which:

- disclose any information relating to management forecasts where this could jeopardise the business effectiveness of the organisation
- or reveal legal proceedings against an individual, except to those directly concerned

1.3 Staff Obligations

The Operations Manager is the Registered Data Controller and is responsible for notification to the Information Commissioner. He/she should be deferred to with any questions relating to data protection or confidentiality. However, **all staff** are responsible for ensuring compliance with this policy. They must:

- Ensure that they have read and understood this policy as it relates to them.
- Ensure that data which they supply or for which they are responsible is up-to-date, accurate, fair and relevant to its purpose, including information about themselves. Staff must notify the organisation of any changes in circumstance to enable the organisation to update personnel records accordingly.
- Not keep any records on other individuals (whether other employees or clients/service users) which are unnecessary, incorrect or which contain unfounded opinion or speculation.
- Not share personal information about other members of staff or clients/service users (e.g. sickness, personal circumstances), that they know as a result of handling confidential information (e.g. sick notes, application forms) or which is disclosed in confidential settings (e.g. supervision or counselling), without that person’s unambiguous agreement.

- Keep data secure. Paper and external computer files must be locked up, computers must be password protected; laptops and computer disks containing personal information, open computer screens, or open paper files must not be left unattended.
- Not disclose, share or transfer outside the organisation any personal information relating to other staff, volunteers, trustees, or clients/service users without the explicit consent of the individual concerned.
- Dispose of personal data safely. Paper notes and records must be shredded or disposed of as 'confidential waste'. Hard drives of redundant PCs must be destroyed or wiped clean before disposal.

Particular care must be taken where personal data is processed 'off-site', at home or in other locations. This presents a greater risk of loss, damage or theft and staff must take appropriate security precautions.

1.4 Guidelines for disclosing information to internal and external sources

Internal information sharing

WiSE recognises that trustees, staff and volunteers may need to share personal information with others internally within WiSE. This might include, for instance, discussion of client issues during supervision, discussion of situations to gain experience and opinion from colleagues, 'on the job' training. Care must be taken that this kind of information sharing is not done publicly or where it can be overheard. Such conversations should wherever possible be held without explicitly identifying the individual or organisation under discussion.

Supervision

Supervision sessions are in general confidential to the Operations Manager and the Trustees of the organisation.

Ground rules for when and why confidentiality may be broken should be agreed at the start of a supervision relationship and might include, for instance:

- information about the progress of work against funding targets
- complex or problematic case management
- discussion of the implications for colleagues of a request for flexible working

- some information to colleagues about personal circumstances which are temporarily affecting performance
- discussion of grievances or concerns about performance with a more senior manager

Wherever possible, agreement about any breach of confidentiality should be reached in advance of the disclosure taking place.

Although the supervisor is bound by confidentiality, it is helpful for the supervisee to inform the supervisor if there are any personal circumstances which are particularly sensitive.

Answering requests for personal staff information

Personal information about a colleague should not usually be discussed with other staff or people outside WiSE without that person's permission. Personal details including address and phone number, health matters or personal circumstances may not be passed on without explicit consent.

It is usually safe to reveal a colleague's work contact (telephone and email address) in response to an enquiry regarding a work function, although these details should not be given to someone wishing to contact a colleague on a non-work related matter.

However, staff must not reveal personal details of other staff members to unknown or unverified external sources, even where these claims to be family members, friends, Government bodies or the police.

Strategies to deal with such enquiries could include:

- Asking the enquirer to put their query in writing or into an email, if appropriate backed up by documentary evidence to support the request.
- Informing the enquirer that a message will be passed on, either asking the person to contact the enquirer directly or agreeing to pass on a sealed envelope/incoming email message to the person.
- Telling the enquirer that you will phone back once you have collected/verified the information required.

1.5 Organisational information

Trustees, staff and volunteers are bound by confidentiality in all matters relating to the internal affairs of WiSE. Confidential information concerning Board meetings, staff meetings, finances, recruitment, planning etc should not be disclosed outside the organisation unless authorisation is given to do so. This does not apply to disclosures made under the Public Interest Disclosure Act ('whistle blowing'). See also Subject Access Requests above.

No statements concerning internal matters or policy may be made to the media without the express permission of the Operations Manager and Chair of Trustees.

WiSE is committed to respecting the confidentiality of those who use and/or support its services. This means respecting the right of members, benefactors, beneficiaries and friends to privacy and their right to expect that any personal information they give us will not be discussed or passed on to anyone outside WiSE without their permission.

Please refer to 'staff obligations' above for general instructions on the collection, use, storage and disposal of all personal information associated with the WiSE

What data?

Personal or sensitive information could include names and addresses, membership details, medical and psychological conditions, financial status, employment status, living arrangements, criminal offences, and internal organisational issues/disputes. The information may be given in conversation or in written form, for example on an application/interview form or email.

Why?

WiSE keeps information on its clients/service users for the purposes of providing a service and meeting client needs.

WiSE will collect names and addresses, including email addresses, of service users for purposes of marketing our services or for quality control purposes. This information will only be used for these purposes with the knowledge and consent of the data subject (see 'Collecting and safeguarding information' below).

WiSE keeps information for applying for funding, monitoring how funds are spent and responding to request for information from Government offices, the Charity Commission and other reputable organisations. Statistical and depersonalised information may be used for campaigning purposes or publicity purposes.

No unrelated data will be kept and any sensitive data held by the organisation will be deleted at the request of the individual concerned.

Where?
All personal data is kept in locked filing cabinets and/or in password protected computer files.

2.1 Recording and accessing information

Written records of any dealings with clients/service users may be made with the client's permission if the purpose of such records is clearly explained to the client. Only essential information should be recorded and these records must be processed in line with Data Protection principles, stored securely and destroyed when no longer needed. Voluntary agreement to supply personal information such as names and addresses will be taken to imply consent to recording that information for WiSE's necessary purposes. [However, where practicable, explicit consent will be sought (or the opportunity to withdraw consent will be offered) on an appropriate letter or form for data protection information].

2.2 Sharing information

Where client information is to be shared with a **partner organisation** or where WiSE is contacting **a third party on the client's behalf**, the client must if possible and practicable confirm their agreement by giving signed authorisation.

Where **funders** require personal information about the beneficiaries of services for audit purposes, this information will be collected on forms which clearly indicate who will receive the information and include provision for service users to sign a consent declaration.

Personal information should not be conveyed to other organisations or individuals via **telephone calls or faxes** without adequate safeguards regarding confidentiality.

External requests for information about an individual should not be sanctioned. Where appropriate, staff may agree to pass on the request to that individual to respond to if they so choose. See advice above for strategies for dealing with requests for information from unknown or unverified enquirers.

Email communications may not be private – please see policy on email and internet use.

Names or contact details should never be released to **the media** in response to requests for ‘case studies’. Media enquiries may, however, be passed on to service users so that they can choose whether to respond to them.

Statistical information may be used for research, monitoring and funding purposes but must not be attributable to an individual. Where, for publicity purposes, WiSE wishes to use an attributed quotation from a client or service user the individual’s express permission must be sought before this can used.

2.3 Collecting and safeguarding information

WiSE also recognises its duty to safeguard the information it holds on external groups and individuals. WiSE will regularly update information, dispose of outdated data and check that storage and archive systems are secure.

All **written materials** applications and packs, registration forms, newsletter forms, training application forms etc] will be designed to ensure that only necessary data is being collected and that this is kept with permission.

If WiSE wishes to use personal information for purposes such as **‘direct marketing’** (e.g. of courses or new services on offer), the organisation will inform the person concerned at the time of collecting the data that it may be used for this purpose. People/organisations will be provided with the opportunity to opt out of being contacted in this way (e.g. by ticking an opt-out box on a form or unsubscribe button).

Mailing and membership lists will only be passed on to other organisations/individuals in order to comply with funding/legal requirements or with the express consent of those listed.

2.4 Subject access requests (SARs)

Any member/user of WiSE is entitled to know what information is held about them, why and where it is held and who can access it. They have the right to see this information and to correct it if necessary. To see information, they should contact the Operations Manager who will arrange a mutually convenient time for this or who will facilitate the involvement of other relevant staff.

3. Exceptions

WiSE reserves the right to break confidentiality if it believes that:

- a child is at risk of being harmed
- a person's life or safety is at risk
- if required by statute (e.g. there is a legal obligation to report drug trafficking, money laundering, terrorist activity to the police)
- if required under a contractual obligation (e.g. where services are purchased by a local authority and that contract requires disclosure of certain information)
- if required by a court order

Information may also be disclosed if the individual concerned has given explicit, preferably written, consent.

Maintaining the confidentiality of identifiable third parties in the course of a 'subject access request' will be considered on a case by case basis.

In all the above cases, the Operations Manager (or if unavailable the Chair or Deputy Chair of Trustees) must be informed immediately.

In other cases, where breaking confidentiality may seem appropriate, this must only be done with the knowledge of appropriate managers or trustees and the person whose confidentiality is to be breached must be informed. They should be informed of their right of complaint and appeal.

Confidentiality Agreement between WiSE (Wetherby in Support of the Elderly) and

Name (please print):

1. I agree to WiSE holding and sharing information about me in line with the Confidentiality, Data Protection and Disclosure Policy.

2. I understand that during my work with WiSE I may learn facts about colleagues or about individuals or organisations with whom WiSE works. I recognise that these facts may be of a personal and confidential nature. I agree not to disclose any such information to any person not authorised by WiSE to hold such information without the express permission of the individual to whom the information pertains, or, in exceptional circumstances, the agreement of my line manager.

3. I agree to uphold this commitment to confidentiality both whilst I am working at WiSE and also in situations outside WiSE.

4 I understand that this does not affect my duty and rights under the Whistle Blowing Policy, Safeguarding Adults and safeguarding Children and Young People policy

Signed: Date:

Related policies

Written Statement of Employment Particulars

Recruitment and Selection

Social Media, Internet and Telephone

Staff Supervision, Appraisals and Development Policy
Whistle Blowing Policy

Relevant legislation

Data Protection Act 1998

Public Interest Disclosure Act 1998