Confidentiality Policy 2023

Last reviewed: April 2023

Next Review: April 2024

Signed (Chair of trustees):

1. Introduction

1.1 The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within St Francis Employability CIO and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

1.2 All employees working for St Francis Employability CIO are bound by a legal duty of confidence to protect personal information they may encounter during their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law Duty of Confidence and the Data Protection Act 1998.

1.3 It is important that St Francis Employability CIO protects and safeguards person identifiable and confidential information that it gathers, creates processes, and discloses, to comply with the law, and to provide assurance to Clients and the public.

1.4 This policy sets out the requirements placed on all staff when sharing information with St Francis Employability CIO and between St Francis Employability CIO and external organisations.

1.5 Person-identifiable information is anything that contains the means to identify a person, e.g., name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted.

1.6 Confidential information with St Francis Employability CIO includes information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including Benefits information, Personal Information etc. It also includes St Francis Employability CIO confidential business information.

1.7 Information can relate to Clients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, mobile phones, digital cameras or even heard by word of mouth.

1.8 A summary of Confidentiality Do's and Don'ts can be found at Appendix A.

1.9 The Legal Framework for confidentiality which forms the key guiding principles of this policy can be found in Appendix B.

1.10 How to report a breach of this policy and what should be reported can be found in Appendix C.

1.11 Definitions of confidential information can be found in Appendix D.

2. Roles and Responsibilities

2.1 The Directors have overall responsibility for strategic and operational management, including ensuring that St Francis Employability policies comply with all legal, statutory and good practice guidance requirements.

2.2 Senior Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon.

2.3 All staff

2.3.1 Confidentiality is an obligation for all staff. There is a Confidentiality clause in their contract and that they are expected to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues.

2.3.2 Any breach of confidentiality, inappropriate use of health, staff records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract and must be reported.

3. Corporate Level Procedures

3.1 Principles

3.1.1 All staff must ensure that the following principles are adhered to: -

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted, or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information must be discussed with either your manager or the Directors.

3.1.2 St Francis Employability CIO is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

3.1.3 Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

3.1.4 Access to rooms and offices where person identifiable or confidential information is stored must be controlled. Doors must be locked. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

3.1.5 All staff should clear their desks at the end of each day. They must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

3.1.6 Unwanted printouts containing person-identifiable or confidential information must be put into a shredded. Discs, tapes, printouts and fax messages must not be left lying around but be filed and locked away when not in use.

3.1.7 Your Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

3.2 Disclosing Personal/Confidential Information

3.2.1 To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

3.2.2 It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

3.2.3 Information can be disclosed:

- When effectively anonymised
- When the information is required by law or under a court order. In this situation staff must discuss with their manager before disclosing.
- In identifiable form, when it is required for a specific purpose, with the individual's written consent.
- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with their manager before disclosing.
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their manager.

3.2.4 If staff have any concerns about disclosing information, they must discuss this with their manager.

3.2.5 Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing/Information Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information see the St Francis Employability CIO Information Sharing Policy.

3.2.6 Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail.

3.3 Working Away from the Office Environment

3.3.1 There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry St Francis Employability CIO

information with them which could be confidential in nature e.g., on a laptop, USB stick or paper documents.

3.3.2 Taking home/removing paper documents that contain person-identifiable or confidential information from St Francis Employability CIO premises is discouraged.

3.3.3 To ensure safety of confidential information staff must always keep them on their person whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be always safeguarded and kept in lockable locations.

3.3.4 When working away from St Francis Employability CIO locations staff must ensure that their working practice complies with St Francis Employability CIO policies and procedures. Any electronic removable media must be encrypted.

3.3.5 Staff must minimise the amount of person-identifiable information that is taken away from St Francis Employability CIO premises.

3.3.6 If staff do need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e., windowless envelope, suitable bag, etc. prior to being taken out of St Francis Employability CIO buildings.
- Confidential information is kept out of sight whilst being transported.

3.3.7 If staff do need to take person-identifiable or confidential information home they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

3.3.8 Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person identifiable or confidential information on a privately-owned computer or device.

3.4 Carelessness

3.4.1 All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes, and other documents.
- Leave a computer terminal, logged on to a system where person-identifiable or confidential information can be accessed, unattended.

3.4.2 Steps must be taken to ensure physical safety and security of person identifiable, or business confidential information held in paper format and on computers.

3.43 Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access the network, this constitutes a disciplinary offence and is gross misconduct which may result in your summary dismissal.

3.5 Abuse of Privilege

3.5.1 It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of GDPR.

3.5.2 When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of St Francis Employability CIO.

3.5.3 If staff have concerns about this issue, they should discuss it with their manager.

3.6 Confidentiality Audits

3.6.1 Good practice requires that all organisations that handle person identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and procedures to evaluate the effectiveness of controls within these systems.

4. Distribution and Implementation

4.1 Distribution Plan

4.1.1 This document will be made available to all Staff via the St Francis Employability CIO internet site.

4.1.2 A global notice will be sent to all Staff notifying them of the release of this document.

4.2 Training Plan

4.2.1 A training needs analysis will be undertaken with Staff affected by this document.

4.2.2 Based on the findings of that analysis appropriate training will be provided to Staff as necessary.

5. Monitoring

5.1 Compliance with the policies and procedures laid down in this document will be monitored on a periodic basis.

5.2 The Resources Manager is responsible for the monitoring, revision and updating of this document on a yearly basis or sooner if the need arises.

6. Equality Impact Assessment

6.1 This document forms part of St Francis Employability CIO commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

6.2 As part of its development this document and its impact on equality has been analysed and no detriment identified.

Appendix A: Confidentiality Dos and Don'ts

Dos

- Do safeguard the confidentiality of all person-identifiable or confidential information that you encounter. This is a statutory obligation on everyone working on or behalf of St Francis Employability CIO.
- Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.
- Do ensure that you cannot be overheard when discussing confidential matters.
- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Do share only the minimum information necessary.
- Do transfer person-identifiable or confidential information securely, when necessary, i.e., use an St Francis Employability CIO email account to send confidential information to another St Francis Employability CIO email account.
- Do seek advice if you need to share person-identifiable information without the client/identifiable person's consent and record the decision and any action taken.
- Do report any actual or suspected breaches of confidentiality.
- Do participate in induction, training and awareness raising sessions on confidentiality issues.

Don'ts

- Don't share passwords or leave them lying around for others to see.
- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don't use person-identifiable information unless necessary, anonymise the information where possible.
- Don't collect, hold, or process more information than you need, and do not keep it for longer than necessary.

Appendix B: Summary of Legal Frameworks

St Francis Employability CIO is obliged to abide by all relevant UK and European Union legislation.

The requirement to comply with this legislation shall be devolved to employees, who may be held personally accountable for any breaches of information security for which they may be held responsible. St Francis Employability CIO shall comply with the following legislation and guidance as appropriate:

The Data Protection Act (2018) and GDPR regulate the use of "personal data" and set out eight principles to ensure that personal data is:

1. Processed fairly and lawfully.

2. Processed for specified and lawful purposes.

3. Adequate, relevant and not excessive.

4. Accurate and where necessary kept up to date.

5. Not kept longer than necessary, for the purpose(s) it is used.

6. Processed in accordance with the rights of the data subject under the Act.

7. Appropriate technical and organisational measures are be taken to guard against unauthorised or unlawful processing, accidental loss or destruction of, or damage to, personal data

8. Not transferred to countries outside the European Economic Area (EEA) without an adequate level protection in place.

Article 8 of the **Human Rights Act (1998**) refers to an individual's "right to respect for their private and family life, for their home and for their correspondence". This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

http://www.legislation.gov.uk/ukpga/1998/42/contents

The Computer Misuse Act (1990) makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer

2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.

3. Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

4. Making, supplying or obtaining articles for use in offences 1-3

http://www.legislation.gov.uk/ukpga/1990/18/contents

- **The duty to share information can be as important as the duty to protect client confidentiality**

Common Law Duty of Confidentiality

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g., a requirement of law or there is an overriding public interest to do so.

Administrative Law

Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is "ultra vires", i.e., beyond its lawful powers.

Appendix C: Reporting of Policy Breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All breaches should be reported to the Manager. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their Line Manager. The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to St Francis Employability CIO systems either by staff or a third party.
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification, and you have concerns that it is not in accordance with the Data Protection Act.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around in public area.
- Theft or loss of person-identifiable or confidential information.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e., disposing off person identifiable information in ordinary wastepaper bin.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager should be sought.

Reporting of Breaches

A regular report on breaches of confidentiality of person-identifiable or confidential information shall be presented to the Directors. The information will enable the monitoring of compliance and improvements to be made to the policy and procedures.

Appendix D: Definitions

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g., name, address, postcode, date of birth, NHS number, National Insurance number etc. Even a visual image (e.g., photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Sensitive/confidential personal information as defined by the Data Protection Act 1998 refers to personal information about: • Race or ethnic origin • Political opinions • Religious or similar beliefs • Trade union membership • Physical or mental health or condition • Sexual life • Commission or alleged commission of any offence, or • Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g., financial reports; commercially sensitive information e.g., contracts, trade secrets, procurement information, which should also be treated with the same degree of care