POLICY:
CONFIDENTIALITY

1. Purpose

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within YANA and have access to personal-identifiable information or confidential information (see appendix C).

All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security. All employees working in YANA are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and data protection legislation – the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA2018) which implements the GDPR in the UK.

It is important that YANA protects and safeguards personal-identifiable and confidential business information that it gathers, creates, processes, and discloses, in order to comply with the law, relevant YANA requirements, and to provide assurance to service users and the public.

This policy sets out the requirements placed on all staff when sharing information within YANA and between YANA and organisations with which it works.

Personal-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.

Confidential information can also include 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 mental health history, employee records, occupational health records, etc.

It also includes YANA confidential business information. Information can relate to service users and staff (including temporary and voluntary 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.

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

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

Definitions of confidential information can be found in Appendix C.

2. Scope

The policy applies to all our employees (including volunteers) regardless of employment agreement or role.

This policy outlines YANA's expectations regarding staff members attitude towards confidentiality.

We promote freedom of expression and open communication, but we expect all staff members to follow our confidentiality policy.

YANA employees are bound by their contract to abide by this Confidentiality Policy while performing their duties. YANA volunteers, under their volunteer agreement, are expected to abide by this Confidentiality Policy whilst performing their role or representing YANA in any capacity.

3. Principles

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

- Personal-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted, or disposed of.
- Access to personal-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 Line Manager or the Charity Manager. YANA is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

Personal-identifiable information, wherever appropriate, in line with the data protection principles stated in the Data Protection Policy, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data in line with the ICO's Anonymisation Code of Practice.

Access to rooms and offices where terminals are present, or personal-identifiable or confidential information is stored, must be controlled.

Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of personal-identifiable information by unauthorised parties.

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

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

YANA's 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

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.

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

- When effectively anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice (https://ico.org.uk/).
- When the information is required by law or under a court order. In this situation staff must raise in the first place with their line manager or the Charity Manager.
- 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 raise in the first place with their line manager or the Charity Manager.
- 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 raise, in the first place, with their line manager or the Charity Manager.
- For any proposed routine disclosures of personal/confidential information, please consult the Charity Manager to see if a Data Protection Impact Assessment should be undertaken.

If staff have any concerns about disclosing information they must raise their concerns in the first place with their line manager or the Charity Manager. Care must be taken in transferring information to ensure that the method used is as secure as it can be.

Data sharing agreements provide a way to formalise arrangements between organisations.

Staff must ensure that appropriate standards and safeguards are in place to protect against inappropriate disclosures of confidential personal data.

It is not permitted to include confidential or sensitive information in the body of an email. When e-mailing to addresses other than secure domains, the information must be sent as an encrypted attachment with a strong password communicated through a different channel or agreed in advance.

When communicating via secure domains, to protect against the risk of accidentally sending to an incorrect recipient, the data should be sent in a password protected attachment, again with the password communicated through a different channel or agreed in advance.

Sending information via email to service users is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent, or the information is not personal-identifiable or confidential information.

3.3 Working Away from the Office Environment

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

To ensure safety of confidential information staff must keep them on their person at all times whilst travelling, out of sight and in the boot of a car, and ensure that they are kept in a secure place at home or if taken to another location.

Confidential information must be safeguarded at all times and kept in lockable locations. When working away from YANA locations staff must ensure that their working practice complies with YANA's policies and procedures.

Any electronic removable media must be encrypted. Staff must minimise the amount of personal-identifiable information that is taken away from YANA premises.

If staff need to carry personal-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 YANA buildings or the usual place of work.
- Confidential information is kept out of sight whilst being transported.

If staff need to take personal-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. It is particularly important that confidential information in any form is not left unattended at any time, for example in a car.

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

3.4 Carelessness

All staff have a legal duty of confidence to keep personal-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 personal-identifiable or confidential information in public places or where they can be overheard.
- Leave any personal-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 personal-identifiable or confidential information can be accessed, unattended.

Steps must be taken to ensure physical safety and security of personal-identifiable or business confidential information held in paper format and on computers. 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. This could also constitute an offence under the Computer Misuse Act 1990.

3.5 Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for, or look at, any personal or confidential information about themselves without a legitimate purpose, unless through established self-service mechanisms where such access is permitted.

Under no circumstances should employees access records about their own family, friends, or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and may be an offence under the Data Protection Act 2018.

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

If staff have concerns about this issue they should discuss it with their Line Manager or the Charity Manager.

Related Documents:

- Declaration of Confidentiality
- Data Protection Policy
- Safeguarding Policy
- Employment Contract/Volunteer Agreement

Revision history

This policy and related guidance will be monitored by the Chair of Trustees/Charity Manager on a regular basis for compliance and will be reviewed at least annually.

Date policy approved or amended	**Amendments**	**Signed**
4 November 2020		
7 December 2021	Updated Policy and Process	E.Haley
October 2023	Reviewed and updated by Kiltti Ltd.	E.Haley

Appendix A:

Confidentiality Do's and Don'ts

Do's

- Do safeguard the confidentiality of all personal-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of YANA.
- Do clear your desk at the end of each day, keeping all non-digital records containing personal-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 personal-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 personal-identifiable or confidential information and ensure they have a need to know.
- Do share only the minimum information necessary.
- Do transfer personal-identifiable or confidential information securely when necessary i.e. use a yanahelp.org email account or password protected attachment.
- Do seek advice if you need to share service user/personal-identifiable information without the consent of the service user/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 personal-identifiable information unless absolutely 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:

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 Charity Manager or the Chair of Trustees. 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 or the Charity Manager.

The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to YANA systems either by staff or a third party. •Unauthorised access to personal-identifiable information where the member of staff does not have a need to know.
- Disclosure of personal-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 and YANA Confidentiality Policies.
- Sending personal-identifiable or confidential information in a way that breaches confidentiality.
- Leaving personal-identifiable or confidential information lying around in a public area.
- Theft or loss of personal-identifiable or confidential information.
- Disposal of personal-identifiable or confidential information in a way that breaches confidentiality i.e. disposing of personal-identifiable information in an ordinary waste paper 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, the Charity Manager or the Chair of Trustees should be sought.

Appendix C:

Definitions

The following types of information are classed as confidential.

This list is not exhaustive:

- Personal-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.

Special categories of personal information (previously known as 'sensitive' personal data) as defined by the Data Protection Act 2018, refers to personal information about:

- Race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- Health data
- Sexual history and/or sexual orientation
- Criminal data

Non-personal-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.