No. 1 Confidentiality Policy

1. Introduction

In the course of their work, trustees, staff and volunteers of For Us Too will obtain and see information about colleagues and external organisations and individuals, particularly disabled children/young people and their families. This policy document provides guidance on how to protect the confidentiality of this information whilst enabling it to be handled according to the requirements of the law, and in the best way possible to support the delivery of For Us Too's aims and objectives.

Please seek advice from the For Us Too Head of Charity or the Chair or Vice-Chair of Trustees if you find anything in this document unclear or you are unsure about how best to protect confidentiality.

2. Scope

This policy applies to:

- For Us Too employees
- Trustees & volunteers
- All contractors and sub-contractors – the charity will ensure that all contracts include a suitable confidentiality clause (see Section 5).

3. Definition

The Collins English Dictionary defines the term confidential as being something:

- "spoken or given in confidence, private; entrusted with another's secret affairs"

Confidentiality is the right of an individual to have personal information, through which they can be identified, kept private. Trust is central to the concept of confidentiality: we must trust colleagues to follow the rules of confidentiality and to be discrete when discussing personal or sensitive information with others both inside and outside For Us Too.

4. The law

The handling of confidential information collected and held by organisations is governed by a number of different Regulations and Acts of Parliament. The following are the most relevant for For Us Too:

General Data Protection Regulation (GDPR) 2018: GDPR came into force in the UK from 25 May 2018 and lays out general rules about data protection. The old Data Protection Act 1998 was a principle-based legal structure and the GDPR continues that approach. This means that rather than a set of rigid rules, the law gives broad principles that will be applied differently by different organisations depending on their circumstances.

The six data protection principles contained in the GDPR are as follows:

- Lawfulness, fairness and transparency
- Purpose limitations
- Data minimisation
- Accuracy
- Storage limitations
- Integrity and confidentiality

Annex 1 sets out how For Us Too has implemented the GDPR within the charity, including data protection principles and provisions.

Human Rights Act 1998: Article 8 gives everyone the right to "respect for private and family life, home and correspondence", unless this is overridden by the 'public interest' e.g. for reasons of Child Protection, for the protection of public safety, public order, health or morals, or for the rights and freedoms of others.

Public Information Disclosure Act 1998: this Act provides protection from victimisation and dismissal to members of staff who speak out ('blow the whistle') against wrong doing at work, including corruption and malpractice. Please see For Us Too's Whistle Blowing policy for more information on this.

As a private organisation, For Us Too is not subject to the Freedom of Information Act 2000.

5. Protecting confidentiality

The following rules on protecting confidentiality apply to all For Us Too employees, trustees and volunteers:

i. Confidential information must not be divulged to another agency or person without the consent of the owner of the information. The only exceptions are where abuse of children or vulnerable adults is suspected (this is developed further in Section 6 below and see For Us Too's Safeguarding and Protecting Children and Vulnerable Adults Policy, Section 10), or there is evidence of other illegal acts, misconduct, serious danger to a staff member or other persons in the community. Such information should then only be divulged to the appropriate authorities after discussion with the For Us Too Head of Charity or the Chair of Trustees as appropriate, who will also determine whether the person to whom the confidentiality is owed will be informed that disclosure has or will be made.

ii. Any disclosure of such confidential information must remain limited to the strict needs of the situation at the time and staff, trustees and volunteers should not assume they have authority to reveal matters which are not relevant to the particular situation.

iii. Any corporate information considered sensitive or confidential to For Us Too must not be disclosed to outside individuals and organisations without the prior agreement of the Head of Charity and/or the Board of Trustees as appropriate. This applies to corporate information essential for the conduct of the charity's business, including the development of strategic objectives, future plans and financial data.

iv. In the course of day-to-day business, For Us Too may need to share anonymised personal & potentially sensitive information with service providers, associated organisations and agents (e.g. Kent County Council) for specific purposes. If there is any doubt that the information can be supplied in accordance with the Data Protection Act and other relevant legislation, the advice of the For Us Too Head of Charity or Chair of Trustees should be sought.

v. Personal or sensitive information must not be disclosed for direct marketing purposes or as part of fund raising.

vi. There may be circumstances where employees, trustees and volunteers would want to discuss difficult or sensitive situations with each other to gain a wider perspective on how to approach a problem, seek advice and ensure a quality service for members and clients. Where possible, discussions should take place without including information that makes the individuals or organisations involved identifiable. If this is not possible, the consent of the organisations or individuals concerned must be sought before discussing the situation, unless there is convincing evidence that the organisation/individual would not object to this i.e. a completed referral form.

vii. Where information is very sensitive, i.e. it involves staff or contractual disputes or legal issues, it will be confidential to the member of staff dealing with the case and the Chair of Trustees. Such information should be clearly labelled 'Confidential' and should state the names of those individuals within For Us Too entitled to access the information and the name of the individual or group who may request access to the information.

viii. Confidential interviews must not be held in places where they can be overheard. No-one should be asked to give personal information in, for example, a rest area, or in a place such as a passage or stairs where it may be overheard by others.

ix. Great care must be taken when discussing confidential information. Colleagues must ensure they are talking to an appropriate person and that they cannot be overheard. If someone takes a call requesting personal information, they should ask the caller if they can return the call and take his or her name and number. Advice on next steps should then be sought from the For Us Too Head of Charity of Chair of Trustees as appropriate.

x. Personal or confidential information gathered from an individual or organisation and intended for an agreed purpose should not be used for another purpose unless the prior agreement of the person or organisation supplying that information is obtained.

xi. Requests for information from the media (e.g. newspapers, TV stations, etc.) about a confidential matter or serious incident (e.g. alleged or suspected child abuse) involving For Us Too must be referred to the For Us Too Head of Charity or Chair of Trustees.

xii. The exchange of personal information or comments (gossip) about individuals with whom For Us Too has a professional relationship should be avoided. It is also not appropriate to discuss a person's sexuality without their prior consent.

xiii. Talking in social settings about organisations or individuals with whom For Us Too has a professional relationship should be avoided.

xiv. Personal, sensitive or confidential information about For Us Too must not be broadcast via the personal social media accounts (e.g. Facebook, Twitter, etc.) of staff, trustees and volunteers. The For Us Too Facebook and Twitter accounts, and the For Us Too website, will never include any information that could be classed as confidential.

xv. Access to For Us Too computers must be password controlled. Passwords must be constructed to minimise the possibility of either being memorised by an onlooker or guessed by a hacker or colleague. They must also be changed at regular intervals or at any time it is suspected that the password has become known.

xvi. Staff members must ensure that personal papers, records relating to members and clients, and other confidential material are kept in a safe place over night e.g. in a locked cabinet or desk drawer. Sensitive material should not be left in places where it may be seen by those not employed by For Us Too.

xvii. When photocopying or working on confidential documents, colleagues must ensure they are not seen by people in passing. This also applies to information on computer screens.

xviii. All records, membership lists, referral files etc. will be reviewed annually and out of date or no longer relevant confidential information deleted.

xix. Membership forms, event forms and photo permission forms will always set out the purpose for which the information is being gathered.

xx. For Us Too staff will ensure that all laptops are properly password protected and stored securely when not in use. Confidential information will not be stored on memory sticks.

Where contractors and employment agencies are used, the contracts between For Us Too and these third parties must contain clauses to ensure that contract staff are bound by the obligations listed above at i. to xx.

6. Safeguarding children & vulnerable adults

Staff, volunteers and trustees have an overriding professional responsibility to share relevant information about the protection of children and vulnerable adults with other professionals, particularly investigative agencies. There must be clear boundaries of confidentiality, however. All personal information regarding a child or vulnerable adult will be kept confidential except when it is suspected that the person may be the victim of abuse.

Where possible, consent should be obtained from the child or vulnerable adult before sharing personal information with third parties. However, in some circumstances obtaining consent may be neither possible nor desirable as the safety and welfare of the person is the priority. For further information, see For Us Too's policy for Safeguarding & Protecting Children & Vulnerable Adults.

7. Access to information

Under the GDPR (see Section 4 above), individuals have the right to receive copies of records held in their name or that of their organisation. Requests must be in writing to the For Us Too Head of Charity giving 14 days' notice and be signed by the individual, or in the case of an organisation's records, by the Chair or Chief Executive of that organisation.

For Us Too employees may have sight of their personnel records held by the charity by giving five days' notice in writing to the Head of Charity or Chair of Trustees as appropriate.

8. Disclosures

We will fully comply with the DBS Code of practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

If it is necessary to keep disclosure information, it will be kept separately from an applicant's personnel file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

In general, a record of basic DBS information will be kept for all staff, trustees and volunteers, including the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

9. Breach of confidentiality

Employee contracts state: "You must not disclose any confidential information arising out of your employment at any time, unless such disclosure is authorised by For Us Too". Employees who breach For Us Too's rules of confidentially will face disciplinary action as set out in the 4us2 Grievance and Disciplinary Policy. Ex-employees breaching the confidentiality rules may face legal action.

Trustees who breach For Us Too's rules of confidentiality will be subject to action determined by the Board of Trustees in accordance with the "Trustee Code of Conduct".

10. Training & Maintaining Confidentiality

The For Us Too Head of Charity will provide staff, volunteers and trustees with annual confidentiality training based on the principles set out in the Kent County Council Common Assessment Framework training modules on confidentiality, the law and child / vulnerable adult protection.
All staff, trustees and volunteers will sign a Confidentiality Agreement (see Annex 2).

Annex 1

General Data Protection Regulation (GDPR) 2018: Implementation

1. Data protection principles

For Us Too is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General provisions

a. This policy applies to all personal data processed by For Us Too.
b. The Head of Charity shall take responsibility for the Charity's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. For Us Too shall register with the Information Commissioner's Office as an organisation that processes personal data.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, For Us Too shall maintain a Register of Systems.

b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by For Us Too must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests - see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ .
b. For Us Too shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in For Us Too's systems.

5. Data minimisation

a. For Us Too shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. For Us Too shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, For Us Too shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. For Us Too shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, For Us Too shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO – see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Annex 2

For Us Too Confidentiality Agreement

For Staff, Trustees and Volunteers

I……agree to this confidentiality agreement, during the entire period of my work / volunteering with For Us Too and also after my role has ended.

I agree that:

- I have read and understood For Us Too's Confidentiality Policy
- I will keep any personal information shared by service users / members confidential, unless they give express permission for me to share it, or the information raises issues of a safeguarding nature
- If I need to share information for safeguarding reasons, I will follow the procedures set out in the For Us Too Safeguarding and Protecting Children and Vulnerable adults Policy
- I understand that the use and disclosure of all information about living, identifiable individuals are governed by the Data Protection Act. I will not use or disclose any personal data I acquire during my work or volunteering for any purpose that is or may be incompatible with the purposes of that work
- I understand that I am required to keep all confidential and personal data securely, and undertake to follow For Us Too's Confidentiality Policy in doing so
- I undertake to ensure that all records provided or created for the purposes of my work / volunteering with For Us Too, including any back-up records, will be passed back to For Us Too or deleted as directed, once I have received confirmation that the work I was employed to do has been satisfactorily completed and all the required information has been provided in accordance with For Us Too's wishes
- I understand that if I choose to stand down from my job / volunteering role I am still expected to keep all shared information confidential at all times

Signed:

Date: