Intercom Trust

Lesbian, gay, bisexual and trans+ people in the South West

Registered charity 1171878

Current version approved: April 2019

Review / refresh due: April 2020

Confidentiality and Information Sharing Policy

1. The Purpose and Implementation of the Policy

1.1. It is important that the Intercom Trust protects and safeguards person-identifiable and confidential business information that it gathers, creates processes, and discloses, in order to comply with the law and to provide assurance to clients and the public. The purpose of this policy is to ensure that the Trust has robust systems in place for protecting confidential and other personal information, in whatever form it is held.

1.2. All staff therefore need to be aware of their responsibilities for safeguarding confidentiality and preserving information security and must participate in training on the subject as requested.

1.3. The officers responsible for the implementation of this Policy shall be the nominated the CEO, the DPO, and other Line Managers. They shall also provide for it to be reconsidered and updated as necessary.

1.4. Line Managers, the DPO, and the CEO will be responsible to the Trustees for actively supervising the implementation of this policy on a day-to-day basis.

1.5. All staff must comply with this policy fully and at all times and must notify the CEO, the DPO, and/or other Line Managers of any breaches of this policy.

1.6. The Trust is registered with the Information Commissioner as a holder of personal data.

2. Confidentiality

2.1. All staff and volunteers of the Trust 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 the Data Protection Act 2018.

2.2. We will make every effort possible in everything we do to comply the following principles:

Lawful, fair and transparent: Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

Limited for its purpose: Data can only be collected for a specific purpose.

Data minimisation: Any data collected must be necessary and not excessive for its purpose.

Accurate: The data we hold must be accurate and kept up to date.

Retention: We cannot store data longer than necessary.

Integrity and confidentiality: The data we hold must be kept safe and secure.

2.3. Our Data Protection Policy outlines our adherence to the principles in greater detail. This Policy specifically relates to how we honour the need to keep person-identifiable information confidential and secure.

2.4. All staff and volunteers of the Trust will regard all information that they may acquire as a result of involvement in the Trust's affairs as confidential to themselves, whether this information be about individuals or organisations.

2.5. Any actual or suspected breaches of confidentiality must be reported to the Line Manager, the DPO, and/or the CEO.

2.6. In dealing with all issues of confidentiality or information sharing the relevant Line Manager, DPO, CEO, and Trustees shall always be guided by legal considerations and best practice for information management.

3. Information Sharing

3.1. The Trust is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

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

3.3. Where necessary the identity of any person who is making a request for person-identifiable or confidential information should be challenged and verified, along with their need to know the information they are requesting.

3.4. If staff have any concerns about disclosing information they must raise in the first place with their relevant Line Manager, the DPO, and/or the CEO.

3.5. Information can be disclosed:

- When effectively anonymised in accordance with the Information Commissioners Office Anonymisation Code of Practice (https://ico.org.uk/).

- In identifiable form, when it is required for a specific purpose, with the individual's written consent.

- 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, the DPO, and/or the CEO.

- When there is a serious safeguarding concern if it is considered that the information required is in a child or vulnerable adult's interest. The Trust will not break any child or vulnerable client's confidence to any external agency or person, including a member of the family, without that client's informed consent, though in cases where there is a clear risk of harm the Trust staff and volunteers must be guided by the provisions of the Trust's Safeguarding Policies. In this situation staff should raise their concerns with their Line Manager, the DPO, and/or the CEO.

- 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, the DPO, and/or the CEO

3.6. Care must be taken in transferring information to ensure that the method used is as secure as it can be. Data sharing agreement can provide a way to formalise arrangements between organisations.

3.7. Be aware that other organisations do not always ensure personally identifiable information is sent securely / encrypted. In these instances staff should highlight this to their Line Manager and may request the organisation involved communicate in adherence with this policy.

4. Information Security

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

Physical Security

4.2. All records on individuals who are not employees (e.g. clients or donors) will be kept as far as possible in dedicated electronic drives on the file server to which staff and volunteers will only have access on a need-to-know basis.

4.3. All paper documents that refer to clients or supporters and cannot be kept in secure electronic form will be kept in a room on the premises which has the highest or second-highest degree of keyed security, in a filing-cabinet which is kept locked at all times when it is not in use.

4.4. All staff should clear their desks at the end of each day and minimise information left out on the desks at all times. In particular they must keep all paper records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

4.5. Access to rooms and offices where terminals are present or person-identifiable or confidential information is stored must be controlled and therefore all doors must be locked when such room are not occupied / in use. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

4.6. Where keys are stored in Keycode boxes, the codes must be returned to 0000 following use.

4.7. No staff or volunteer may be issued with a key which provides access to a room or a filing cabinet which they do not need for the performance of their duties.

4.8. Staff should ensure that they cannot be overheard when discussing confidential matters.

4.9. When printing personal-identifiable information from an office computer into an unsecure environment (e.g. reception), these should be collected immediately and not left unattended in the reception area.

4.10. All employment files will be kept in secure folders on the file server and (in respect of paper records) in a secure locked cabinet on the premises, in the room which has the highest degree of keyed security. Only the CEO and individuals nominated by the trustees will have direct access to these folders and files.

4.11. All employees have a right to see the contents of their own personnel file. No employee or volunteer other than the nominated Line Manager, the CEO, the Chair, Secretary and Treasurer of the Board of Trustees has a right to have access to any employment file that is not their own.

Electronic Security

4.12. Staff should switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if they leave their desk for any length of time.

4.13. 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.

4.14. All passwords for secure electronic storage, such as drives or Outlook folders, must be known to the CEO and to Trustees or other trusted individuals nominated by the Board.

4.15. No confidential material may be synchronised to a Trust-owned laptop, a tablet, or copied onto a memory stick or any other removable media without express permission from the Line Manager, DPO, or CEO. Encryption and / or password protection must be used in such circumstances.

4.16. 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

4.17. Appropriate back-up and disaster recovery solutions shall be in place.

Email / Outlook Security

4.18. It is not permitted to include confidential or sensitive information in the body of an email.

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

4.20. All confidential information, other than that mentioned above, must only be emailed via an approved encryption service or as an encrypted attachment with a strong password.

4.21. To protect against the risk of accidentally sending to an incorrect recipient, any confidential data sent in a password protected attachment must have the password communicated through a different channel or agreed in advance.

4.22. All personal contact-data for individuals who are known to the Trust only as individuals (i.e. not through any work with our stakeholder or partner organisations or as customers or suppliers) will be kept in dedicated Outlook Contacts folders to which staff and volunteers will only have access on a need-to-know basis.

Out of the Office

4.23. If staff need to take person-identifiable or confidential information away from the office 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.

4.24. It is particularly important that confidential information in any form is not left unattended at any time, for example in a car, unless safely locked in the boot at all times and not left there overnight.

5. Data Retention

5.1. No personal data should be retained which the Trust does not have a right to retain and a purpose in retaining.

5.2. It is important to ensure that person-identifiable data on individuals outside the Trust is held no longer than is necessary, and that any request from a data subject to disclose, amend or remove the information we hold is acted on promptly. All such requests must be passed on to the Line Manager, the DPO and/or CEO.

5.3. Support and Advocacy client records will be retained for at least six years, but during the retention period, the case file should not be used or consulted save for internal monitoring evaluation or scrutiny purposes, and then only with the authorisation of the Line Manager, the DPO, the CEO or a Trustee.

5.4. Employment records will be retained as long as is best practice at the time.

5.5. When data has exceeded its retention date this should be reported to the Line Manager, the DPO, or CEO, who may—at their discretion, and bearing in mind the legal requirements at the time—authorise a senior member of staff to securely shred the data and / or securely delete it from the electronic system.

6. Abuse of Privilege

6.1. It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information about 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 the Data Protection Act 2018.

6.2. Any breach of confidentiality, inappropriate use of client data, 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 to an appropriate Line Manager, the DPO, and/or the CEO.

7. Freedom of Information

7.1. Freedom of Information legislation does not apply to the Trust. The Act only applies to public authorities.

7.2. If a request is received by the Trust for disclosure of documents of any kind that cites this Act, the Trust will refuse the request as a matter of policy, explaining that the legislation does not apply.