Intercom Trust

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

Registered charity 1171878

Current version approved: February 2022

Review / refresh due: February 2023

Confidentiality, Information Security and Information Sharing Policy

1. The Purpose and Implementation of the Policy

1.1. It is important that 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 Intercom 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 Deputy Director, and other Line Managers. They shall also provide for it to be reconsidered and updated as necessary.

1.4. Line Managers, the Deputy Director, 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 Deputy Director, and/or other Line Managers of any breaches of this policy.

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

2. Data Protections & Confidentiality

2.1. All Intercom staff and volunteers 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. We must therefore be very clear with our clients, in an age appropriate and understandable manner, about what information we record about them and why, what we will (or could) do with it, and their rights within in.

Limited for its purpose: Data can only be collected for a specific purpose. At Intercom this is for the purposes of providing our services. We must not use identifiable client information for any other reason.

Data minimisation: Any data collected must be necessary and not excessive for its purpose. This means that we should not record or share information about a client that is not necessary for the purposes of provided our service to them.

Accurate: The data we hold must be accurate and kept up to date. This means that we need to take care to ensure that the information we keep is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.

Retention: We cannot store data longer than necessary. It is useful to keep some client information for a while after they have stopped using our services. However, we should ensure that we are very clear about our last point of contact with a client so that we can delete / destroy this information when the retention period is over.

Integrity and confidentiality: The data we hold must be kept safe and secure. Information security and safety is an utmost priority for us and must be at the forefront of our minds and informing our practice at all times. Whenever we contemplate or adjust how we manage information, we must think about data protection and design this into the process from the start.

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 Intercom Trust will regard all information that they may acquire as a result of involvement in Intercom'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 Information Governance Lead, and/or the CEO.

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

3. Information Security Procedures

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

3.2. Pseudonymisation is used at Intercom to assist us to keep client details secure. At the first possible instance, a client is given a SID number (generated by the ITC database) which is then used in any calendars, boards, or internal communications. This helps us to keep a client's name safe.

Physical Security

3.3. 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.

3.4. 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.

3.5. 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.

3.6. 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.

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

3.8. 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.

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

3.10. 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.

3.11. 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 Deputy Director and individuals nominated by the trustees will have direct access to these folders and files.

3.12. 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 Deputy Director, 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.

Network Security

3.13. Intercom's internal network will be available when needed, can be accessed only by legitimate users and will contain complete and accurate information.

3.14. The network must also be able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this we undertake to:

- Protect all hardware, software and information assets under its control;
- Provide effective protection that is commensurate with the risks to its network assets;
- Implement the Network Security Policy in a consistent and timely manner;
- To comply with all relevant legislation.

3.15. Capacity to access any physical aspect of the server will be restricted and only managed through specific permission by the CEO.

3.16. Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network will conform to specific security procedures.

3.17. We will ensure that all users of the network are provided with the necessary security guidance, awareness and training to discharge their security responsibilities.

3.18. Data backup procedures are outlined in the Business Continuity Plan document.

3.19. We will ensure that measures are in place to detect and protect the network from viruses and other malicious software.

3.20. We will ensure that where equipment is being disposed of all data on the equipment (*e.g.* on hard disks or tapes) is securely overwritten.

3.21. Network Security Policies, design documentation, security operating procedures and network operating procedures.

Electronic Security

3.22. Access to any information held on computer, laptop, mobile phone, or our Server is restricted by user as appropriate to their role. Access will be granted or revoked upon changes to employment status. This is the responsibility of the line manager.

3.23. 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.

3.24. Computers are set to automatically install relevant updates, and staff should double-check that this is done on a regular basis.

3.25. 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.

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

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

3.28. Staff must not forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not access, use, or store person-identifiable or confidential information on a privately-owned computer or device without explicit permission from the CEO and having signed an additional security agreement.

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

Email / Outlook Security

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

3.31. 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.

3.32. 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.

3.33. 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.

3.34. All personal contact-data for individuals who are known to Intercom 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

3.35. 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.

3.36. 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.

3.37. It is crucial that no Intercom device is attached to a public WiFi at any time. This includes laptops and mobile phones. Home WiFi may be used only where appropriate passwords and security measures are implemented. WiFi provided by other professional services may be used with permission of the line manager.

4. Information Sharing

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

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

4.3. 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.

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

4.5. 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 Information Governance Lead, 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. Intercom 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 Intercom staff and volunteers must be guided by the provisions of the Intercom's Safeguarding Policies. In this situation staff should raise their concerns with their Line Manager, the Information Governance Lead, 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 Information Governance Lead, and/or the CEO

4.6. 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.

4.7. 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.

5. Data Retention

5.1. No personal data should be retained which Intercom 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 Intercom 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 Deputy Director and/or CEO.

5.3. Support and Advocacy client records will be retained for 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 Deputy Director, 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 Deputy Director, 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. Individual Rights

6.1. Individuals have the legal right to object to how we keep our information or what we do with it, to request access to their data, to rectify it in case of errors, to erase it, to restrict what we use it for, and to reuse it for their own purposes. More information on these rights and how to support people to enact them can be found in our Data Protection Policy.

6.2. The Privacy Notice for Individuals should be made available to individuals wherever appropriate as this explains this information to clients.

6.3. It is crucial that those we work with understand what we record and why as well as what their rights are in relation to it. Explanation of this should be managed on a person by person basis, based on ensuring appropriate understanding. Explicit and evidenced, informed consent for us to record and use their information is preferable at every point, but may be impractical at times, for example in Helpline calls.

7. Subject Access Requests

7.1. An individual has the right to receive confirmation that their data is being processed, access to their personal data and supplementary information which means the information which should be provided in a privacy notice.

7.2. We must provide an individual with a copy of the information the request, free of charge. A form for Subject Access Requests is available in the Policies & Procedures Folder.

7.3. This must occur without delay, and within one month of receipt. We endeavour to provide data subjects access to their information in commonly used electronic formats, and where possible, provide direct access to the information through a remote accessed secure system.

7.4. If complying with the request is complex or numerous, the deadline can be extended by two months, but the individual must be informed within one month. You must obtain approval from the Information Governance Lead before extending the deadline.

7.5. We can refuse to respond to certain requests, and can, in circumstances of the request being manifestly unfounded or excessive, charge a fee. If the request is for a large quantity of data, we can request the individual specify the information they are requesting. This can only be done with express permission from the Information Governance Lead.

7.6. Once a subject access request has been made, you must not change or amend any of the data that has been requested. Doing so is a criminal offence.

8. Freedom of Information Requests

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

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

9. Abuse of Privilege

9.1. 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.

9.2. 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 Deputy Director, and/or the CEO.

10. Confidentiality Audits

10.1. Audits will focus primarily on control within electronic records management systems but also include paper record systems and confidentiality processes, for example secure transfers of information processes. The purpose is to discover whether confidentiality has been breached or put at risk through deliberate misuse of systems as a result of weak, non-existent or poorly applied controls.

10.2. Confidentiality audit checks will be carried out using a variety of methods. Types of Confidentiality Audits may include:

- Monitoring of incident reports and near misses
- Spot-checks of IT security, physical security measures, disposal arrangements, off-site records management,
- Complaints from members of the public / staff
- Failed log-in reports and password changes provided for information systems
- Checks to ensure staff understanding and awareness of IT security, information access, reporting incidents, and Data Protection and Confidentiality Policies and procedures

10.3. The CEO, as Caldicott Guardian and SIRO, has overall responsibility for the monitoring incidents and complaints relating to confidentiality breaches, for ensuring that access to confidential information is regularly audited, and for ensuring recommendations and concerns arising from confidentiality audits are actioned within a reasonable timeframe.

10.4. The Deputy Director, Intercom's Information Governance Lead, is responsible for carrying out audits and spot-checks as required and for highlighting any reported breaches or near misses to the CEO. They are also responsible for implementing improvements as directed.

10.5. Line managers are responsible for ensuring that staff for whom they are responsible are aware of their responsibilities with regard to confidentiality of information and ensure that staff complete relevant training. Line managers are also responsible for ensuring that their staff are fully aware of the mechanisms for reporting actual or potential confidentiality breaches.

10.6. All staff have a duty to read and work within current policies. They should ensure that confidential information is not accessed without prior authorisation and completion of the appropriate documentation. Confidential information should also not be disclosed to unauthorised recipients.

I have read and understand this policy, and I undertake to observe it carefully at all times.

Signed: _____ Date: _____

Name _____

Signature of supervisor or volunteer co-ordinator: _____

Name: _____