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

Data Protection Policy

1. The Purpose and Implementation of the Policy

1.1. Intercom Trust hold personal data about our clients, employees, suppliers and other individuals for a variety of relevant purposes. Intercom is committed to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

1.2. The purpose of the Data Protection Policy is to support the 7 Caldicott Principles, the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

1.3. This policy sets out how we seek to protect personal data and ensure that our staff understand the rules governing their use of the personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Chief Executive (CEO), the Deputy Director (Information Governance Lead), the Caldicott Guardian Trustee and/or a member of staff nominated by the Trustees be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

1.4. This policy applies to all personal data processed by Intercom Trust.

1.5. Staff will receive adequate training on GDPR and provisions of data protection law specific for their role. Staff must complete all training as requested. If you require additional training on data protection matters, contact the CEO, the Deputy Director, or your line manager.

1.6. 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.

1.7. 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.

1.8. 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.

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

2. Data Protection Principles

2.1. The Intercom Trust is committed to processing data in accordance with its responsibilities under the GDPR. We shall make every effort possible in everything we do to comply with the principles of data protection (the Principles) enumerated in the General Data Protection Regulation.

2.2. The Principles are:

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.

3. Lawful, fair and transparent processing

3.1. Our commitment to the this Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

3.2. Intercom Trust maintains an Information Asset Register, containing this information. The Information Asset Register shall be reviewed at least annually.

3.3. We must ensure that individuals whose data is being processed by us are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy notice. This applies whether we have collected the data directly from the individual, or from another source.

3.4. Individuals have the right to access their personal data and any such requests made to Intercom Trust shall be dealt with in a timely manner.

4. Limited for Lawful purposes

4.1. All data processed by Intercom Trust must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).

4.2. Intercom Trust shall note the appropriate lawful basis in the Information Asset Register.

4.3. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.

4.4. 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 the Intercom Trust's systems.

Special Category Data

4.5. Previously known as sensitive personal data, this means data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination.

4.6. Where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

4.7. The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

Criminal Offence Data

4.8. All data relating to criminal offences is considered to be a special category of personal data and must be treated as such.

4.9. Criminal record checks cannot be undertaken based solely on the consent of the subject. DBS checks are justified by law.

5. Data Minimisation

5.1. Intercom 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. Data Accuracy

6.1. Intercom shall take reasonable steps to ensure personal data is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained.

6.2. 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. Retention, Archiving, and Removal

7.1. To ensure that personal data is kept for no longer than necessary, Intercom has in place a Records Retention Schedule, defining each area in which personal data is processed and the length of time such records should be kept.

7.2. When personal data is deleted this should be done safely such that the data is irrecoverable.

8. Security

8.1. Intercom shall ensure that personal data is stored securely using modern software that is kept-up-to-date and in locked cabinets stored within locked offices. Access to personal data shall be limited to personnel who need access and appropriate security must be in place to avoid unauthorised sharing of information.

8.2. The Confidentiality and Information Sharing Policy has further information about how we safeguard the confidentiality of personal information.

9. Breach

9.1. All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures

- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

9.2. 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, a Breach of Data Protection Form must be completed. A form for Breach of Data Protection is available in the Policy & Procedure Folder.

9.3. Intercom shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

9.4. Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

10. Individual Rights

10.1. Individuals have rights to their data which we must respect and comply with to the best of our ability.

10.2. We must ensure individuals can exercise their rights in the following ways:

Right to be informed

- Providing privacy notices which are concise, transparent, intelligible and easily accessible, free of charge, that are written in clear and plain language, particularly if aimed at children.

- Keeping a record of how we use personal data to demonstrate compliance with the need for accountability and transparency.

Right of access

- Enabling individuals to access their personal data and supplementary information

- Allowing individuals to be aware of and verify the lawfulness of the processing activities

Right to rectification

- We must rectify or amend the personal data of the individual if requested because it is inaccurate or incomplete.

- This must be done without delay, and no later than one month. This can be extended to two months with permission from the Information Governance Lead.

Right to erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

Right to restrict processing

- We must comply with any request to restrict, block, or otherwise suppress the processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further. We must retain enough data to ensure the right to restriction is respected in the future.

Right to data portability

- We must provide individuals with their data so that they can reuse it for their own purposes or across different services.
- We must provide it in a commonly used, machine-readable format, and send it directly to another controller if requested.

Right to object

- We must respect the right of an individual to object to data processing based on legitimate interest or the performance of a public interest task.
- We must respect the right of an individual to object to direct marketing, including profiling.
- We must respect the right of an individual to object to processing their data for scientific and historical research and statistics.

Rights in relation to automated decision making and profiling

- We must respect the rights of individuals in relation to automated decision making and profiling.

- Individuals retain their right to object to such automated processing, have the rationale explained to them, and request human intervention.

11. Privacy Notices

11.1. Privacy notices must be concise, transparent, intelligible and easily accessible. They are provided free of charge and must be written in clear and plain language, particularly if aimed at children

11.2. The following information must be included in a privacy notice to all data subjects:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place
- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the ICO, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

12. Subject Access Requests

12.1. 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.

12.2. 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.

12.3. 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.

12.4. 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.

12.5. 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.

12.6. 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.

13. Third parties

Using third party controllers and processors

13.1. As a data controller and data processor, we must have written contracts in place with any third party data controllers and/or data processors that we use. The contract must contain specific clauses which set out our and their liabilities, obligations and responsibilities.

13.2. As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

13.3. As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Contracts

13.4. Our contracts must comply with the standards set out by the ICO and, where possible, follow the standard contractual clauses which are available. Our contracts with data controllers and/or data processors must set out the subject matter and duration of the processing, the nature and stated purpose of the processing activities, the types of personal data and categories of data subject, and the obligations and rights of the controller.

13.5. At a minimum, our contracts must include terms that specify:

- Acting only on written instructions
- Those involved in processing the data are subject to a duty of confidence
- Appropriate measures will be taken to ensure the security of the processing
- Sub-processors will only be engaged with the prior consent of the controller and under a written contract
- The controller will assist the processor in dealing with subject access requests and allowing data subjects to exercise their rights under GDPR
- The processor will assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches and implementation of Data Protection Impact Assessments
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information necessary for the controller and processor to meet their legal obligations.
- Nothing will be done by either the controller or processor to infringe on GDPR.

14. Audits, monitoring and training

Data audits

14.1. Data audits may be carried out to manage and mitigate risks will inform the information asset register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.