Data Protection Policy 2018

Policy statement

INQUEST is committed to practices and procedures that ensure information relating to service users, employees, trustees, volunteers, employee applicants, supporters and partners is treated in the utmost confidence. Everyone involved with the organisation is expected to be aware of their responsibilities regarding the information they come across.

Due to the sensitive nature of the work of INQUEST, breach of the data protection and confidentiality policy may be grounds for disciplinary action or, in the case of volunteers and trustees, a review of their relationship with the organisation.

The purpose of this policy is to enable INQUEST to:

- Comply with the law, including the General Data Protection Regulation (GDPR), and good practice in respect of the data it holds about individuals;
- Protect INQUEST's service users, employees, volunteers and other individuals and respect their rights;
- Provide training and support for staff and volunteers who handle personal data, so that they can act confidently and consistently;
- Protect the organisation from the consequences of a breach of its responsibilities.

INQUEST recognises that its first priority under GDPR is to avoid causing harm to individuals. Information about staff, volunteers and service users will be used fairly, securely and not disclosed to any person unlawfully.

The relevant legislation aims to ensure that the legitimate concerns of individuals about the ways in which their data may be used are taken into account. In addition to being open and transparent, INQUEST will seek to give individuals as much choice as is possible and reasonable over what data is held and how it is used.

Any queries regarding data protection that are not answered by this policy, or accompanying procedures, can be answered by INQUEST's Data Protection Officer, the Operations Director.

Scope of the policy

This policy applies to all employees (permanent and temporary), volunteers (including trustees), agency workers, consultants, contractors, partners, supporters and visitors.

Overview of the General Data Protection Regulation

GDPR, introduced in 2016, is an EU directive on data protection that supersedes the Data Protection Act 1998. The deadline for introducing the principles of GDPR is 25th May 2018; from this date onwards, INQUEST will adhere to all relevant principles and legal requirements.

Under GDPR, all personal data that INQUEST collects must be:

- collected only for specified, explicit and legitimate purposes, and that the manner in which the data is collected is compatible with those purposes,
- limited to what is necessary for and relevant to the purposes that it serves,
- accurate and up-to-date,
- kept in a form which identifies its subject for no longer than necessary and
- processed in a secure manner – this includes protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

Under GDPR, INQUEST, as the controller of the data that it collects and stores, shall be responsible for, and be able to demonstrate, compliance with the above principles.

Definitions

GDPR applies to both data controllers and data processors. The former determines the purpose and means of processing personal data and ensures that data processors are compliant in GDPR. The latter process data on behalf of a controller; GDPR applies to all data processing work undertaken by data processors.

The data subject, or 'subject', is the individual whose personal data is being processed. Subjects include, but are not limited to: current and past employees, volunteers, job applicants, donors and service users.

Data processing means the use made of personal data including:

- obtaining and retrieving
- holding and storing
- making available within or outside the organisation
- printing, sorting, matching, comparing, destroying.

Personal data is defined as any information relating to an identifiable person who can be directly or indirectly identified by that data. This applies to both manually recorded data and automated data.

The Data Protection Officer is the name given to the person in organisations who is the central point of contact for all data compliance issues at INQUEST.

Responsibilities

The Board of Trustees recognises its overall responsibility for ensuring that INQUEST complies with its legal obligations.

The Data Protection Officer is currently Operations Director, Arnaud Vervoitte, who is responsible for:

- briefing the board on data protection responsibilities,
- reviewing data protection and related policies,
- informing and advising other staff on GDPR and other data protection legislation and related issues,
- ensuring that data protection induction and training takes place,
- handling subject access requests as well as requests to transfer, rectify and erase personal data,
- approving unusual or controversial disclosures of personal data,
- ensuring contracts with data processors have appropriate data protection clauses, electronic security and
- approving data protection-related statements on publicity materials and letters.

As a non-profit organisation, INQUEST is exempt from registering a Data Protection Officer with the Information Commissioner's Office, however if this exemption is removed, INQUEST will register.

Each member of staff and volunteer at INQUEST who handles personal data will comply with the organisation's operational procedures for handling personal data (including induction and training) to ensure that good data protection practice is established and followed and that all data protection practice is lawful.

All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

Significant breaches of this policy, and failure to report them, will be handled under INQUEST's disciplinary procedures.

Lawful basis for processing

There are six lawful bases[1] for processing personal data. From 25th May 2018, all data must have a lawful basis for processing identified by INQUEST staff that collect or process it. In every case of personal data processing, INQUEST will clearly state the lawful basis in its data processing and this will be communicated to the individuals affected.

In addition to a lawful basis for processing data, processing any special category data[2] requires an additional condition. Special category data includes, but is not limited to: race, health and sexual orientation.

See the Lawful Basis Procedure for further detail on how to ensure that you are acting within the law with regard to lawful bases, criminal offence data and special category data.

Confidentiality

Because confidentiality applies to a much wider range of information than data protection, INQUEST has a separate confidentiality policy. The two policies should be read in conjunction.

Staff, volunteers and sessional workers are required to sign a short statement indicating that they have been made aware of their confidentiality responsibilities.

In order to provide some services, INQUEST may need to share a client's personal data with other agencies (third parties). Verbal or written agreement will be sought from the client before data is shared.

If anyone within INQUEST feels that it would be appropriate to disclose information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this will only be done after discussions with a manager or the Data Protection Officer. All such disclosures will be documented.

Governance and accountability

INQUEST will demonstrate their compliance with the accountability principle of GDPR through mandatory staff training, annual updates (and further ad hoc updates in line with legislation) of this policy and related procedures and, where possible, data minimisation and pseudonymisation/anonymisation.

---

[1] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

[2] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

Third party processors (including consultants) will have appropriate GDPR regulations[3] included in their contract with INQUEST so that INQUEST, as the data controller, can ensure compliance.

As an organisation of fewer than 250 employees, INQUEST will not actively document all of its processing activities. INQUEST will, however, in line with the GDPR exemption for small organisations, document all processing activities that are:

- not occasional – this means anything out of the ordinary,
- could result in a risk to the rights and freedoms of individuals or
- involve the processing of special categories of data or criminal conviction and offence data.

If the exemption for small organisations is removed or changed, INQUEST will have the ability to demonstrate that it documents all of its processing activities during the course of 2018.

Furthermore, INQUEST staff will support INQUEST's Data Protection Officer in undertaking an annual internal audit[4] in to what personal data is held and what that data is used for. This audit will be authorised by the Executive Director and signed off by the Board of Trustees. To make this process more straightforward, INQUEST recommends that its projects undertake more regular audits of their data. This audit will document:

- INQUEST's Data Protection Officer,
- the purposes of INQUEST's data processing,
- a description of the categories of individuals and categories of personal data processed,
- categories of recipients of personal data,
- details of transfers to third parties and the safeguards for transfer mechanisms,
- retention schedules,
- a description of INQUEST's technical and organisational security measures and
- a record of any breaches.

Data protection impact assessment

INQUEST staff will undertake a data protection impact assessment[5] (DPIA) for any processing that is likely to result in a high risk to individuals' interests. High risk processing includes that of special category data or criminal data *on a large scale (where large scale may include duration of the processing)*, processing personal data without providing the individual with a privacy notice or processing personal data which, in the case of a breach, may result in physical harm. The Data Protection Officer's advice will be sought when completing a DPIA. If a processor decides not to complete a DPIA, the Executive Director's permission must be obtained.

If a DPIA is undertaken and a high risk is identified which cannot be mitigated, the Information Commissioner's Office must be consulted.

---

[3] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

[4] https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

[5] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

There is no INQUEST DPIA procedure; any DPIA must be undertaken using the advice of the Information Commissioner's Office[6].

Security and data storage

INQUEST will undertake appropriate technical and organisational measures to process personal data securely.

Any personal data will be:

- Kept in securely, if in physical copy,
- Protected by the use of passwords, if kept on a computer,
- Destroyed in an appropriate manner, if it is no longer needed and
- Stored in as few places a possible (staff and volunteers are discouraged from establishing unnecessary, new data sets)

Access to personal data stored on the incumbent main database is controlled by a password; only those needing access are given the password.

INQUEST stores archived paper records of clients and volunteers securely in the office.

INQUEST's contract with its IT provider, Them Digital, will be GDPR compliant; this includes ensuring that INQUEST's IT systems have GDPR-compliant cybersecurity measures.

Staff and volunteers should be careful about information that is displayed on their computer screen and make efforts to ensure that no unauthorised person can view the data when it is on display. The security measures of INQUEST's office include locks.

INQUEST staff and volunteers are required to not use commercial WiFi to access work systems (including WiFi in cafes and public transport).

Notes regarding personal data of clients should be shredded or destroyed.

If any of these measures are found to be insufficient, INQUEST will increase security measures where relevant. Security measures will be tested and updated when the data protection policy is updated, annually. The test will be organised and overseen by the Data Protection Officer.

Data Retention

The following table shows the retention schedules for types of data that INQUEST processes. The table refers to the length of time at which data should be deleted from all INQUEST storage (including paper).

Data category	Retention schedule	Notes

[6] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Staff and volunteers (including trustees') data	7 years after the staff or volunteer terminates their work with INQUEST	This is a legal requirement
Financial documentation	6 years after the end of the previous financial year	This is a legal requirement
Service user data	As long as necessary (case closure processes will be determined for each project separately)	This is to ensure that the data is kept long enough to process it for INQUEST's advice work, research and policy work and projects' reporting requirements

If a member of staff processes a category of data that is not accounted for in the table, either speak to the Data Protection Officer to discuss adding that data category to the policy or – if that data processing is likely to be a one-off, seek the advice of the Data Protection Officer regarding its retention time and record the results of the discussion for future reference.

If any data subject requests the erasure of their data, please follow the procedure in the Subject Access Request procedure, which in most situations will overrule the data retention policy.

Breaches

A personal data breach means a breach of security leading to the unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, whether accidental or deliberate.

Data breaches will be acted upon in line with INQUEST's Data Breach Procedure which follows the legal requirements of GDPR.

Subject access requests, data rectification and data erasure

All individuals whose personal data is processed by INQUEST have the right to request:

- access to all information stored about them (a 'subject access request');
- that their data transferred to another electronic service ('the right to data portability');
- that their personal data is rectified;
- that their data erased or;
- that the use of their personal data restricted.

In a majority of cases, INQUEST will need to comply with that individual's request. See the Subject Access Request Procedure for further detail on what to do upon receipt of such a request, including time limits.

Privacy Notice

All data subjects will be given the GDPR-compliant INQUEST privacy notice at the same time as their data is first processed. INQUEST staff will recommend that all service users read the Privacy Notice. All data subjects will be given an opportunity to read the privacy notice before their personal data is transferred to a third party.

For data subjects whose first contact with INQUEST is over the phone, INQUEST staff will inform clients of their right to read the privacy notice and tell clients how to access the notice. If a client would like to read a hard copy of the privacy notice, INQUEST will send a paper copy to the client at no charge.

If a new data subject's data is given to INQUEST by a third party, INQUEST will seek to give the data subject the privacy notice within one month of processing their data.

Consent

Under GDPR all personal data processing that takes place under the lawful basis of 'consent'. In practice, this is unlikely to affect those who work with service users as service users' data will be generally be processed under the lawful basis of 'legitimate interests'. It does, however, mean that no direct marketing (including but not limited to seeking donations and promoting INQUEST's services and events) can take place without consent which explicitly allows for those forms of direct marketing.

INQUEST will provide to individuals whose data is being processed the following information:

- the purpose of processing their data,
- the lawful basis of processing their data and, if that basis is of 'legitimate interests', what those legitimate interests are,
- what categories of personal data will be obtained, if it is not obtained directly from the subject,
- details of transfers to any third parties, where applicable,
- the retention period of the personal data,
- the rights available to the subject regarding the processing their personal data and
- the right to lodge a complaint regarding the processing of their personal data and to withdraw consent.

If any information about service users, staff and volunteers is made public, further consent will be sought, in line with GDPR's requirement to seek consent for every new data processing purpose. Consent for using clients' data to show INQUEST's impact will, in general, not be sought as fully anonymised data does not fall under GDPR. If the impact data is not fully anonymised, consent will be sought from those who it identifies.

Consent can be withdrawn at any time. If an individual wishes to withdraw consent retrospectively, they will need to request that INQUEST erases or edits their data, as described under the sub-heading 'subject access requests, data rectification and data erasure'.