Number One Community Trust

Data Protection & GDPR Policy (Draft)

Policy Statement

The protection of data of individuals working with and visiting Number One Community Trust is very important to staff and trustees. We will only gather information about individuals to help improve and extend the services we offer and to keep people safe and informed. We will ensure its protection by adopting the following policy and maintaining a legal position.

Purpose of Policy

Number One Community Trust will comply with the Data Protection Act 1998 (DPA), which sets out the law regarding the processing of personal data. This policy and the guidance notes attached clarify Number One Community Trust's expectations of staff and volunteers with regards to the processing of personal data. Personal data means information that relates to a living individual who can be identified from the information.

For detailed support and advice on Data Protection visit:
http://ico.org.uk/for_organisations/data_protection/the_guide

This policy and the accompanying guidance notes will be kept under review and will be subject to revision from time to time.

Scope of Policy

This policy and procedure applies to all employees and volunteers who process personal data at Number One Community Trust.

The Data Protection Act (DPA) was introduced to ensure that organisations keep personal data secure and use it only for the purposes for which it was given. Individuals enjoy rights regarding the way their personal information is handled, and all organisations have a duty to ensure those processing personal data on their behalf understand what they need to do and have access to appropriate support and advice.

The DPA requires organisations to manage data according to some simple principles. In summary personal information must be:

- processed lawfully and accurately;
- processed only for specified purposes;
- be kept secure, accurate and up to date;
- be relevant, not excessive and retained for no longer than necessary;
- be processed in accordance with the rights of the individual whose personal information is being processed

Data Security

Data security is one of the most important areas of the DPA. In respecting the personal data for which it is responsible, Number One Community Trust expects staff and volunteers to ensure that:

- Computers, laptops, mobile phones and PDAs are kept password protected at all times and locked when not in use, with screen locks enabled if left unattended. Passwords should not be shared or left visible;
- Data and equipment such as laptops or PDAs are never left vulnerable, particularly in public places;
- Data that would compromise individuals or Number One Community Trust if lost must not be transported on USB sticks or CD ROMs unless relevant encryption software has been activated.
- All staff, volunteers, members and young people's details forms are kept under lock and key in Number One Community Trust offices. They are not kept at home or left on desks or on fax/copying machines at any time. If copies are made, these should be kept securely and shredded as soon as possible.
- After visits or meetings, personal data is taken or sent securely to Number One Community Trust offices as quickly as possible and preferably on the same day, and removed from mobile devices such as laptops immediately;
- All Participant Detail Forms sent between Number One Community Trust and Delivery Partners should only be sent by Recorded Delivery.
- Papers, CDs and discs containing personal data should only be sent by registered post or by secure fax.
- Personal data sent by email to external addresses that would cause distress, loss or embarrassment if mislaid, wrongly directed or compromised must be password-protected and encrypted.
- Records kept on the CRM or in other electronic locations must only contain factual, accurate and up to date information. No data without a business case is retained.

Monitoring of emails

Number One Community Trust reserves the right, in certain circumstances, to access the emails of staff who are absent on leave or unwell. Access is restricted, and requests for access must be approved by the Chairman of the Board of Trustees.

These principles are covered in more detail in the guidance notes. All staff and volunteers are required to adhere to the information provided therein.

Data Protection Guidance Notes

This guide covers all the principles, and puts them in four simple sections:

1. Data collection and usage

2. Data quality

3. Individuals' rights and other requests for access

4. Data security, storage, destruction and retention.

Data Collection & Usage

This covers the first two principles:

Data shall be:

- Processed lawfully and accurately; and

- Processed only for specified purposes

When Number One Community Trust collects personal data, (for example, when people fill in application forms to join activities) it must make it clear how it is going to use this information. Accordingly, forms that collect information must include what is known as a fair collection notice (FCN).

The FCN describes how the information will be used and, where appropriate, provides the individual with the option to opt out of receiving further contact from Number One Community Trust. Number One Community Trust **cannot** use the information provided in any other way, without notifying the individual first to get their permission.

Sensitive personal data

There is certain data that is sensitive, and special rules apply to it.

The categories of sensitive data are:

- Racial or ethnic origin
- Political opinion
- Religious or other similar beliefs
- Physical and mental health
- Sexual life
- Any proceedings for any committed or alleged offences

To process this type of data Number One Community Trust must have **explicit consent**. This means it must get the individual to sign that they are content that their data is collected and processed. Again, Number One Community Trust must be clear how the information will be used can be used. This also includes data captured as part of case study material for publication.

Younger Participants

Whilst those aged twelve and over are considered of sufficient age and maturity to understand their rights under Data Protection legislation, care should be taken to ensure that they do clearly understand what they are signing, the meaning of the FCN and the implications of giving their consent. If there are any concerns about an individual young person's ability to understand, or where the young person is less than twelve years of age then consent must be sought from their parent, carer or guardian.

Data Quality

This covers the next three principles:

Data shall be:

- Kept accurate and up to date
- Relevant and not excessive
- Retained for no longer than necessary

Accurate and Up to Date

Number One Community Trust wants to ensure that all stored data is accurate and up to date. In order to comply, staff may choose to send a regular mailing to clients, or contact them by telephone,

to ensure their data is correct. It is up to management to determine how often this is done, but as a good practice, this would be a minimum of once every two years.

Number One Community Trust will therefore undertake regular reviews of its data to identify any mistakes and, where possible, correct them. Where this is not possible, inaccurate records must be removed.

Relevant and not Excessive

Number One Community Trust only collects personal data that is relevant to its purpose. Staff and volunteers should avoid the temptation of recording anything in excess of this. Only collect what is going to be used – if you don't need it, don't record it.

Opinions as well as facts are covered by the Data Protection Act. Great care should be made by all staff and volunteers to record facts and not opinion. People have a right to ask to see the information held about them.

Keeping Information Longer than Necessary

Number One Community Trust must be able to demonstrate that it needs the information it holds; information no longer required for funding or operational purposes should be destroyed. Paper files should be retained in accordance with retention guidelines.

Before employees or volunteers leave, it is the responsibility of management to ensure the files they leave behind are relevant, up to date and accurate.

Individuals Rights

Data shall be:

- Processed in accordance with the rights of the individual whose personal information is being processed

The DPA provides people with rights in relation to the processing of their personal information. These rights are:

- the right to obtain a copy of the information about them, plus a description of the type of information being processed, the uses that are being made of the information and those persons to whom their personal information has been disclosed
- the right to withdraw consent
- the right to have inaccurate information about them corrected
- the right to object to direct marketing
- the right to claim compensation where they have suffered damage or distress as a result of a breach of the DPA

1. *The right to obtain a copy of the information about them*: At any time, anyone can contact Number One Community Trust to request to see information held about them. This information may be held on computer, archives, email or in paper-based files. All such requests must be made in writing to Number One Community Trust. The Chair of Trustees should be notified if a request of this kind is received.

2. *The right to withdraw consent*: Any person, donor or supporter can contact Number One Community Trust and request that it ceases to process their personal data. This is known as withdrawal of consent. Those wishing to do so must write to Number One Community Trust with the reasons why they wish use of their data to cease. A response must be sent within twenty-one days. The Chair of Trustees should be notified if a request of this kind is received.

3. *The right to have inaccurate information corrected*: Number One Community Trust should ensure records are accurate and up to date and do not contain inaccurate or erroneous statements or opinions. Under the DPA, anyone is entitled to compensation where they have suffered damage due to unlawful data processing. That means they can sue Number One Community Trust. If anyone approaches Number One Community Trust to have their details corrected, appropriate action should be taken.

4. *The right to object to direct marketing*: People have the right to decide whether or not they wish their information to be used for direct marketing purposes. Number One Community Trust offers the option to "opt-out" of receiving marketing materials. Anyone can opt-out at any time and Number One Community Trust must respect this and amend records to ensure mailings by e-mail and/or post no longer continue.

Other Requests for Access

Sometimes Number One Community Trust may be contacted by third parties who would like access to client records.

a) The Police

If the police contact you for data, you should confirm with the police that the reason for the request is that they wish to contact a named individual about a named criminal investigation (regardless of whether that individual is a suspect or witness) and that failure to release the data would prejudice the investigation. Most police forces will have their own request form which should always include a statement confirming that the information requested is required for the purposes covered in Section 29 of the Data Protection Act, a brief outline of the nature of the investigation and the subject's role in that investigation, and the signature of the investigating officer. This document must be obtained prior to the release of any information. All requests from the Police should be sent to the Chair of Trustees for approval and prior to action being taken.

b) Other third parties

If Number One Community Trust is approached with a request for information about a data subject from any other third party the following approach should be taken.

Number One Community Trust only considers approaching a data subject if releasing information will be in their interest. Number One Community Trust needs to get written consent from the data subject allowing the information to be released. The data subject needs to know as much information about the request as possible so that they can make an informed decision as to whether they are willing to let the information be released. The request details should be recorded. This criterion includes parents who wish to see data. Even if a parent or guardian was present at the time the data was collected, consent from their child is required before releasing information to them. There are instances where Number One Community Trust can proceed without consent and these requests should be considered on a case by case basis.

c) Court Order

If a request for disclosure through Court Order is received, the Chair of Trustees should be notified.

d) Research purposes

Occasionally a company or a funder may wish to use Number One Community Trust data for research purposes. If clients have given consent through the FCN, this can proceed. This is not always the case and advice should be sought before data is released, if in doubt.

Sharing Information

As a rule of thumb, data can only be shared with the individual's consent. There are occasions where it may be necessary to share information without consent. Examples of these occasions are where, in the immediate circumstances, it is not possible to obtain it beforehand or because it might prejudice the purposes for which the information is being disclosed. Number One Community Trust will consider every request on a case by case basis.

Examples:

- The individual is at risk of harm, needs urgent medical treatment, or may harm someone else.
- The disclosure prevents an individual committing a criminal offence that could put others at risk or place a member of staff or any other person at risk of accusations of collusion.
- If the organisation is ordered to provide information as part of legal proceedings – such as when solicitors require to employment records as part of litigation claims against Number One Community Trust or requests from the police above.
- To protect children, young people or vulnerable adults from abuse.

Collecting data or buying from Third Parties

This refers to situations where Number One Community Trust might buy in mailing lists, for example. Number One Community Trust should obtain confirmation that the party providing the information has the consent of the person to whom the information relates and to ask to see the FCN. If this cannot be confirmed, then do not collect the data. Number One Community Trust does not sell its data. If it intends to share it with other organisations, the FCN must make this clear.

Data Security, Storage and Destruction

This covers the final principle, that data shall be kept secure.

Secure Storage and Handling

Number One Community Trust has a responsibility to everyone to ensure that they can have complete confidence that the information they give us will be treated with respect. This means files are kept locked away when not in use. Paperwork is not left out overnight or at unattended desks. This includes staff records, including performance reviews and other personal information. Only those staff and volunteers who need to have access to data in order to carry out their roles should have access to it.

Manual Records

Manual records are those containing information about clients, employees and volunteers that are not held on computer. These files fall within the regulations of the DPA, as they are considered relevant filing systems. Relevant filing systems are defined as "any set of information relating to individuals to the extent that the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to an individual is readily accessible". Even if files are recorded by a number they will have, as part of the referencing system, a method to identify the individuals concerned.

All manual records kept in Number One Community Trust offices are kept in secure filing cabinets.

Manual records kept by volunteers or by staff working at home must be kept in secure filing cabinets and should contain only the most recent client contact data, all other records should be kept in the office file. A record of files kept in home offices must be kept in Number One Community Trust offices.

Access to manual files should be restricted to named staff and volunteers. One member of staff should have responsibility for files and hold the keys to the cabinets. This responsibility will include knowing where files are if they are not in the filing cabinet.

Where files are taken out of the office, best practice would recommend that files are logged in and out, with a return date. Those logging files out are personally responsible for the file until it is returned. A maximum log out time should be 2 weeks. Files not returned in time must be tracked down. A log should also be kept where files have been copied. Photocopies of documents should be shredded after use.

Files should never be left in unattended vehicles.

When staff or volunteers leave, management must ensure that all files and records are returned for central filing or destruction.

Computer records

All Number One Community Trust computers are password protected. This means that even if a laptop is stolen only someone knowing the password will be able to access Number One Community Trust data. It is imperative that passwords are kept secret and should not be shared with anyone, even family or other staff.

It is an individual's responsibility to safeguard information held on personal IT equipment in the same way as paper files held at home. Such information must be transferred to Number One Community Trust equipment at the earliest opportunity and deleted from personal equipment.

Access to the Number One Community Trust databases is restricted to designated and trained staff only.

Any request for data to be emailed must be appropriately authenticated and sent securely. If in doubt, do not send it.

Verbal leaks

All staff members and volunteers should be informed that they need to be careful not to disclose information about clients, however inadvertently. Number One Community Trust has a Confidentiality Policy and all staff and volunteers should be made aware of its contents.

Archiving records

All records that need to be kept for a designated or extended period of time (for example; contract related evidence) must be stored in a secure archive location. Archived materials must be listed so that records can be retrieved if required. Computer records should be backed up onto CD ROM disks/USBs and then archived. The CDs/USBs should then be placed with the relevant paper files and archived with them.

Destruction

Files no longer required must be destroyed. This should be done as follows:

- Paper files must be shredded or incinerated. Any paper files in the possession of volunteers must be brought into the office for destruction. When records are destroyed by external storage companies a certificate of destruction is issued, these should be kept and filed.
- Deleting information from computers - Each individual system is set up with protocols for managing data including destruction. Where Number One Community Trust no longer has any business use for data it should be deleted from systems.
- Computer discs and CDs must be wiped clean of data and completely destroyed. No Number One Community Trust computers can be sold or disposed of until they have been professionally wiped clean of data. On leaving Number One Community Trust, staff and volunteers must return all equipment they have in their possession.

GDPR

General Data Protection Regulation (GDPR) came into place on 25 May 2018. It is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).

The GDPR principles are broadly similar to the principles in the Data Protection Act 1998 (the 1998 Act) setting out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

The key changes are:

- there is no principle for individuals' rights. This is now dealt with separately in Chapter III of the GDPR;
- there is no principle for international transfers of personal data. This is now dealt with separately in Chapter V of the GDPR; and
- there is a new accountability principle. This specifically requires an organisation to take responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate that compliance.

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Number One Community Trust values the trust of individuals working with and visiting the centre, as such it taking responsibility for GDPR compliance by putting in place appropriate technical and organisational measures to meet the requirements of accountability including:

- adopting and implementing a data protection policy
- where appropriate, putting written contracts in place with organisations that process personal data on your behalf
- taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations
- maintaining documentation of your processing activities
- implementing appropriate security measures
- recording and, where necessary, reporting personal data breaches
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests
- adhering to relevant codes of conduct and signing up to any certification schemes
- regularly reviewing and updating accountability measures as necessary aligned to the Data Protection Policy