Hartley Wintney Voluntary Care Group

Serving the Community since 1977

Data Protection Policy

As part of the Good Neighbours Network (GNN) we recognise that colleagues need to collect and use certain types of information (personal data) about individuals and organisations in order to carry out our work. We recognise our duty of care to use this information lawfully and fairly. We understand that this personal information/data must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the General Data Protection Regulations 2018 (GDPR).

Personal Data

Personal data is anything that identifies a living person such as:

- Name, address, telephone number, email address
- Financial information
- National insurance number
- Birth certificate, passport, driving licence
- CCTV images, voice recordings
- Sensitive details - religion, ethnic origin, health records, politics, trade union membership, genetics, biometrics (for ID purposes), sex life or sexual orientation*

*We understand that the above named sensitive details are subject to additional conditions that need to be applied before we can use them. Explicit consent is usually needed before we can share these details or pass them onto others.

There are times when our duty of care requires that we do share personal data, i.e. if an assessment of risk to an individual has been identified. We understand that it does not matter how data is obtained; information provided via the internet, email, social media, post/written comments can all be classed as personal data.

Why and How Data Is Held

Most information held by us relates to community organisations, volunteers, committee members and clients. We are clear on the legitimate/lawful need for recording and maintaining the personal information for individuals, i.e. we cannot undertake the activity on behalf of our clients or volunteers without this information.

In order to comply with the principles of GDPR, we understand that personal information about individuals, whether on a computer or on paper, falls within the scope of data protection and must comply with the principles for data protection.

Personal data must be:

- Obtained and processed fairly and lawfully
- Held only for specified legitimate purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept secure and protected
- Not kept longer than necessary for legitimate purposes
- Processed in accordance with the Act

Data Processing

The data processor is any individual who is recording and working with personal data. Data processing includes:

- Recording and updating personal details
- Recording information from telephone calls
- Reviewing/reading a file/document (paper or electronic)
- Storing/archiving/destroying a file/document (paper or electronic)
- Discussing any action that needs to be taken
- Creating/receiving emails or other correspondence

All processing has to meet at least one of a set of 6 conditions called 'legal bases:

- Consent of the data subject
- In connection with the contract
- In order to comply with the law
- In an individual's 'vital interests'
- In the public interest
- In your 'legitimate interests'.

Personal Data Communication

We understand that we have a legitimate interest to capture personal data for our volunteers and clients, and that this can be demonstrated (i.e. help cannot be given without the capture of the contact details for a volunteer or client). The key points of why we need to hold their personal data need to be pointed out to an individual at the time of data capture (on the telephone or face to face) with a Short Hand Privacy Notice and the individual must be informed as to how they can access a Full Privacy Notice. A data subject can challenge this legitimate interest and if this occurs, we will need to provide compelling reasons for keeping this data. We understand that we must be clear on our legitimate interest and that at no time must this override the fundamental rights and freedoms of the data subject.

Privacy Notices

We will ensure that every data subject is made aware of how to access a Full Privacy Notice, which explains the legitimate interest/lawful basis for maintaining our clients' and volunteers' personal data, our data retention period and that individuals have a right to complain to the Information Commissioner's Office (ICO) if they think there is a problem with the way we are handling their data. This Full Privacy Notice will enable us to identify ourselves to individuals and how we intend to use their personal data. This notice will be need to be concise, easy to understand and written in clear language. We will also use shorter privacy notices, as appropriate.

Rights of an Individual (Data Subject)

We understand that under the new GDPR rules, all individuals will have new rights in relation to how their personal information is processed and held by organisations and that some of their existing rights will be strengthened.

These rights now include:

Right to be informed We understand that we will inform individuals of our intention to process and hold their personal information. We understand that we will also need to tell individuals why we wish to hold their personal information, where it will be stored and for how long. We will also need to

advise individuals of their rights and who they can contact for more information on their rights under GDPR. We understand that we will make use of both short hand and longer version to inform individuals of their rights.

Right of access We understand that individuals now have the right to access the personal information that we already hold on them. We will ensure that we follow a Subject Access Request (SAR) procedure to supply a copy of an individual's personal information within **a month.**

Right to be forgotten We understand that individuals will now have the right to request that we delete their personal information without undue delay. We understand that we may also have to notify third parties (such as public sector or other voluntary organisations) of the individual's request to be forgotten.

Right to rectification We understand that individuals will now have the right to have inaccurate personal information held about them rectified without undue delay.

Right to object to processing of personal information by a group We understand that an individual has the right to object to processing on the basis of their particular situation, in addition to the right to object to direct marketing.

Right to complain to the 'supervisory authority' We understand that an individual has the right to complain to the ICO and have this complaint investigated.

Subject Access Requests

We understand that a 'Subject' (sometimes also known as a 'Data Subject') is a person – an employee, a volunteer, client or committee member who can be identified. We understand that this 'Subject' may request access to data that is held about them and they have a right to know what we have and to see it. We understand that procedures already in place should be updated and a plan made on how to handle requests taking into account the new GDPR rules:

- In most cases we will not be able to charge for complying with a request
- We will have **a month** to comply
- We can refuse or charge for requests that are manifestly unfounded or excessive
- If we refuse a request, the individual must be told why and that they have the right to complain to the supervisory authority and to a judicial remedy
- They (the Data Subject) will need to prove who they are

Reporting Data Breaches under GDPR

We understand that if data is accidentally or deliberately lost or shared, this is called a data breach. We understand that we will regularly review the procedures we have in place to detect, investigate and report a personal data breach. We understand that anybody can make a mistake but that it is the duty of an individual who is responsible for a breach to report this immediately to the relevant person.

We understand that GDPR has now introduced a duty to report data breaches to the ICO. We will notify Good Neighbours Network Hub staff, in addition to the ICO, within **72 hours** (or explain why we are late) if a data breach has been identified where it results in a risk to the rights of the individual. We understand that failing to report a data breach within **72 hours** (or explain why we are late) could mean that we could be fined. We understand that a breach of security is anything that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise.

We understand that there are fines for **not** reporting and that they apply now to all organisations not just government organisations, so it is important that we report any breach swiftly should it happen. We understand that we should assess the types of personal data we hold and document where we will be required to notify the ICO or affected individuals if a breach occurs.

Examples of Data Breaches Can Include:

- Loss or theft of data or equipment
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances
- Hacking
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

Keeping Records

We will ensure that all colleagues are committed to ensuring data protection responsibilities are actioned and reviewed on a regular basis and that we view data protection as an integral part of all project planning and meetings. We will ensure that we take appropriate measures to comply with and importantly to demonstrate that we are complying with data protection law. We should ensure that we only keep personal data for as long as we need it to undertake our activities.

These will include:

- Setting up all new projects/reviewing existing projects with data protection focus
- Team meeting minutes where data protection is discussed
- GNN sample documents (fit for purpose and followed)
- Staff induction, supervision and training
- Records of monitoring, audits and reviews
- Records of incidents (how handled and what was learned)