# Confidentiality and Data Protection Policy

This policy was reviewed and approved by the Management Committee at the AGM on 24th April 2023. The policy was reviewed and amended to comply with the General Data Protection Regulation (GDPR), effective from 25th May 2018.

It will be reviewed in 2026

## 1 Introduction and definitions

The Iver Good Neighbours Scheme (IGNS) is committed to protecting the confidentiality and personal data of everyone it works with, and especially our volunteers and service users (i.e. our neighbours and clients).

IGNS will comply with the General Data Protection Regulation (GDPR), which is the set of legal rules governing the processing and control of personal data. It covers the storage, use and transfer of information relating to living individuals who can be identified.

IGNS recognizes and respects the individual rights (as described in the GDPR – Appendix 1) of those whose personal data it collects, stores and processes.

IGNS will adhere to the guiding principles of the GDPR (Appendix 2)

**Key roles described by the GDPR are:**

**Data Controller** – the Management Committee of IGNS is the Data Controller and determines the way personal data is collected, and its purposes, within the Scheme. It is accountable for this data and for adhering to, and demonstrating compliance with, the data protection principles. It should be proactive and reactive to any concerns raised, as well as regularly reviewing Privacy Policies, Procedures and Notices. It will ensure all our volunteers are aware of their rights and responsibilities and can comply with the values and good practice expected of IGNS volunteers.

**Data Protection Officer** – this is the person responsible within the organisation for data protection compliance. He or she will be appointed by the IGNS Management Committee at the AGM annually and will report directly to them.

**Data Processor** – volunteers within the Scheme who process data on behalf of the Committee. Other Data Processors include our Phone System host; Internet Service Providers; Website host and 'cloud storage' platforms. We will ensure procedures with each of these to secure personal data.

**Data Subject** – anyone with personal information stored about them within the Scheme.

**General principles**

IGNS will collect the minimum amount of personal information that is necessary to meet the requests made by users of the service.

Data subjects will be informed about the intended use of their personal data, the length of time it will be retained and the reason for these.

The lawful basis for IGNS processing personal data is that individuals have given their clear consent to IGNS processing their relevant personal data for one or more specific purpose.

Consent must be a freely given, specific, informed and unambiguous indication of the individual's wishes. The data subject has the right to withdraw their consent at any time.

Consent must be a clear affirmative action – a positive 'opt-in' by data subjects.

All personal data must be accurate and up to date, **insofar as notification of changes are given to the Scheme by the Data Subject.** Old or inaccurate data will be erased or corrected.
All personal data will be stored safely and securely for as long as it is needed to meet the wishes of service users and volunteers – and consent is positively given.

All personal data will be deleted when it is no longer required, or when consent is withdrawn.

Volunteers will be given induction training, which will cover all policies and procedures, including those covering Confidentiality and Data Protection.

Volunteers can share information anonymously with a duty co-ordinator, to discuss relevant options, issues and seek advice.

No one should share personal information or comments (gossip) about volunteers or individuals with whom the Scheme is working.

No personal information will be shared with a third party, without the consent of the data subject.

Where there is a legal duty on IGNS to disclose information (for example, where there are safeguarding concerns), the individual will be informed that disclosure has or will be made.

**Why information is held.**
Personal information held by the IGNS relates to volunteers, neighbours (i.e. service users) and other services, organisations or people that support or fund them.
Information is necessary to enable IGNS to respond positively to requests received from neighbours.
Anonymous aggregated data about age, gender, ethnicity, disability and employment status of users may be kept for the purposes of monitoring our equal opportunities policy and for reporting back to funders.
IGNS volunteers and neighbours are informed that we intend to hold their personal data on the Scheme laptop, which is shared between Duty Coordinators. They must consent to this.

**Access to information**
Data subjects have the right to know what data is held on them, why the data is being processed and whether it will be given to a third party.
Data subjects have the right to access this information and to be given it in hard copy. They also have the right to have personal data deleted – the right to be forgotten.
If someone asks for a copy of their data (known as a **subject access request**), IGNS will provide the information within one month, having verified the identity of the person making the request.

Personal information about a service user will only be shared with a volunteer or co-ordinator who is working directly with that neighbour. No personal information about the volunteer will be given to the service user, other than their name.
Sensitive personal data (e.g. information relating to racial, health, political or sexual identity) can only be processed with the specific, positive and free consent of the data subject, and then only if it is relevant and necessary to achieving their wishes.
All Data Subjects have the right to complain to the Information Commissioners Office if they have a problem with the way we have handled their data. (Appendix 3)

**Storing information**
All hard copies of confidential information must be kept in a locked filing cabinet or lockable box file.
The Scheme laptop and any memory stick holding personal data must be kept in a safe place, preferably a locked room or cabinet. The Scheme laptop is password protected.
Personal information that identifies a data subject (neighbour or volunteer), shared by email in the course of IGNS business, must be deleted from the volunteer's computer as soon as possible.

**Duty to disclose information**

There is a legal duty to disclose some information including:
Adult safeguarding concern, which will be reported to the Social Services Department (See IGNS Safeguarding Adults Policy and Procedures).
Drug trafficking, money laundering, acts of terrorism or treason, which will be disclosed to the police.

**DBS Disclosures**
As an organisation using the Disclosure and Barring Service (DBS) to help assess the suitability of volunteers for positions of trust, IGNS complies fully with the DBS Code of Practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.
Disclosure information is kept securely, in lockable storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties.

In accordance with section 124 of the Police Act 1997, Disclosure information is only passed to those who are authorised to receive it in the course of their duties.

Disclosure information is only used for the specific purpose for which it was requested and for which the applicant's full consent has been given.

Once a recruitment decision has been made, we do not keep Disclosure information for any longer than is necessary. This is generally for a period of up to six months, to allow for the consideration and resolution of any disputes or complaints.

Once the retention period has elapsed, we will ensure that any Disclosure information is immediately destroyed by secure means, i.e. by shredding, pulping or burning. We will not keep any photocopy or other image of the Disclosure or any copy or representation of the contents of a Disclosure. However, we will keep a record of the date of issue of a Disclosure, the name of the subject, the unique reference number of the Disclosure and the details of the recruitment decision taken.

**Data Breaches**

A data breach is a breach of security leading to 'accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data'.

IGNS is developing procedures to detect, investigate and report a personal data breach and to demonstrate the measures it has in place to protect against a data breach.

When the Data Protection Officer becomes aware that a data breach has occurred, he or she will notify the Management Committee (i.e. Data Controller) and a judgment will be made as to the type and level of risk and what action is required e.g. notification of Information Commissioner's Office (Appendix 4); notification of those directly concerned. Notification will take place within 72 hours if as a result of the breach there is a risk to the rights and freedoms of individuals, which, if unaddressed, could have a significant detrimental effect on the individual e.g. discrimination; reputational damage; financial loss; or, loss of confidentiality. Where it is a 'high risk' loss the data subjects will be notified directly.

The impact of the breach will be assessed on a case-by-case basis to decide whether the loss is significant and meets the thresholds for notification.

Any volunteer, duty co-ordinator or management committee member who breach any of the conditions within this policy will be dismissed from IGNS.

**Appendix 1**

**Individuals' rights under the GDPR**

- the right to be informed.
- the right of access.
- the right to rectification.
- the right to erasure.
- the right to restrict processing.
- the right to data portability.
- the right to object.
- the right not to be subject to automated decision-making including profiling.

**Appendix 2**

**GDPR Data Protection Principles**

Lawful, fair and transparent

Specified, explicit, legitimate purpose – information collected on one basis cannot be used for another

Adequate, relevant, limited – no more information than is necessary to conduct business; Goldilocks principle 'just right'; info cannot be collected 'just in case'; 'Justify it' – must be able to explain; Data minimisation – data deleted when no longer required

Accurate and up to date – clear out old, correct and erase

For no longer than is necessary – data retention policy

Handled securely – apply technological and organisational measures for the lifetime of the information.

**Appendix 3**

**Information Commissioners Office**

Email: https://ico.org.uk/global/contact-us/email