



Saint John of God Housing Association CLG

**Board Directors/Members,
Staff & Tenants**

Data Protection Policy

Approved by the Board of Directors



Saint John of God Housing Association CLG

Data Protection Policy

Document Reference Number:	SJOG HA 05	Document drafted by:	Planning & Development Manager
Revision Number:	Version 1	Document Approved by	Board of Directors
Approval Date:	July 2018	Responsibility for implementation:	Chief Executive Planning & Development Manager All HA
Revision Date:	July 2020	Responsibility for evaluation and audit:	SJOG Housing Association
		Number of Pages:	22



Saint John of God Housing Association CLG

Data Protection Policy

Contents

1. Policy Statement	7
2. Policy Purpose	7
3. Scope of the Policy	8
4. Definition of Data Protection Terms.....	8
5. Data Protection Principles.....	9
6. How are the data protection principles applied by Saint John of God Housing Association?	10
7. What obligations must Saint John of God Housing Association staff members comply with?	11
8. How can staff members ensure that data is kept safe?	12
9. Providing Information over the telephone.....	15
10. How does Saint John of God Housing Association manage personal data queries?	15
11. Subject Access Requests.....	15
12. Third Party Processors	16
13. Data Breaches.....	16
14. Personal Data Breach	17
15. Data Loss Incident Logging	19
16. Enforcement	19
17. Review of Policy	20
18. References	20



Saint John of God Housing Association CLG

Data Protection Policy

1. Policy Statement

Everyone has rights with regard to how their personal data is handled. This Policy sets out the obligations of Saint John of God Housing Association clg ("The Housing Association") under data protection law and how that commitment is carried out with regards to the collection and use of personal data. Data protection law safeguards the privacy rights of individuals as well as laying down responsibilities for the processing of personal data. Data Protection law imposes restrictions on how the Housing Association may collect and process that data.

It is intended that by complying with these guidelines, the Housing Association will adhere to best practice under Data Protection law.

In the course of its operations, the Housing Association is required to collect and use certain information and use certain types of information about people, including 'personal data' and 'special categories' of data as defined by the General Data Protection Rules (GDPR).

2. Policy Purpose

The Housing Association must comply with the data protection principles set out in the General Data Protection Regulation (GDPR)¹. The Policy sets out the rules and the legal conditions that must be satisfied in relation to the collecting, obtaining, handling, processing, storage, transportation and destruction of personal data.

¹ The General Data Protection Regulation (GDPR) will come into force on the 25th May 2018, replacing the existing data protection framework under the EU Data Protection Directive.

3. Scope of the Policy

The Policy applies to all personal data and sensitive data collected, processed and stored by The Housing Association in relation to its employees, service providers and tenants ("Data Subjects") in the course of its day to day activities. Data can be held by The Housing Association in paper form or electronic form.

The Policy applies to all members of staff, including contractors and temporary personnel, who process personal data as part of their work. The Housing Association treats the rights of all Data Subjects equally, whether they are employees, tenants or suppliers.

Effective Date: 26th May 2018

4. Definition of Data Protection Terms

Data is information which is stored electronically, on a computer, or in paper files. This includes IT systems and CCTV systems.

Data Subjects include all living persons about whom The Housing Association holds personal data.

Personal data means is data relating to a living person who is or can be identified, either from the data or from the data in conjunction with other information that The Housing Association holds as a Data Controller. Personal data can be simple facts (such as a name, address or date of birth) or it can be an opinion (such as a staff performance review).

Data Controller is the individual or organisation who controls and is responsible for the keeping and use of data. The Housing Association is a Data Controller.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following the Policy at all times.

Processing means doing anything with the data. There is a long list of examples of processing set out in GDPR. Some examples include collecting, recording or keeping data, using the data or destroying the data.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, criminal convictions or the alleged commission of an offence. Sensitive personal data can only be processed under strict conditions, and usually requires the consent of that person in order to process it.

5. Data Protection Principles

The Housing Association staff must deal with all personal data in a responsible manner and in accordance with the following eight Data Protection principles which state that data must be:

1. Obtained and processed fairly
2. Used only for the purpose that it was gathered in the first instance
3. Kept safe and secure
4. Accurate and up to date
5. Disclosed only in line with the original purpose
6. Not excessive but relevant and adequate
7. Retained only for as long as needed for the original purpose
8. Presented to Data Subjects on request

Source: Data Protection Commissioner <https://www.dataprotection.ie>

6. How are the data protection principles applied by Saint John of God Housing Association?

In the course of its daily organisational activities, The Housing Association acquires, controls, processes and stores personal data of Data Subjects. Data Protection law imposes restrictions on how The Housing Association may collect and process that data. When gathering personal data The Housing Association must state its reasons for looking for it, what it will be used for and who it will be shared with. The Housing Association must ensure that any data collected is limited to what it actually needs, for purposes which are specific, lawful and clearly stated.

Before The Housing Association processes any personal data it must tell Data Subjects that they have a right to complain if they are unhappy with the reasons for processing and what rights they have under GDPR. The Housing Association must ensure that it uses technical measures & have procedures in place to secure the personal data against unauthorised access, unlawful process or accidental loss or damage.

Where possible, The Housing Association will seek the consent of the Data Subject before their data is processed. Where it is not possible to seek consent, The Housing Association will ensure that collection of the data is justified under one of the other lawful processing conditions set out under GDPR, for example, legal obligation, for a contract etc.

As The Housing Association is a landlord, it collects personal data to create a tenancy agreement with a tenant. The Housing Association processes the personal data of tenants so that it can manage the tenancy, for example, liaising with tenant for payment of rent, organising repairs, dealing with tenant issues or complaints etc.

As an employer The Housing Association collects personal data of its staff to create an employment contract. The Housing Association processes the personal data of staff in order to pay wages, and maintain a personnel file through the HR Department at Saint John of God Hospitaller Ministries HQ. There is a data sharing agreement in place between Saint John of God Housing Association and Saint John of God Hospitaller Ministries.

Access to and management of staff and tenant records is limited to those staff members who have appropriate authorisation.

The Housing Association must also comply with statutory obligations and under some laws The Housing Association can be obliged to share personal data of Data Subjects, for example, to the Residential Tenancies Board to register a tenancy, or to An Garda **Síochána** where a crime has been committed.

Where The Housing Association intends to record activity on CCTV, a notice will be posted in full view. For further details on the use of CCTV, see our CCTV policy.

If you visit our Website to browse, read or download we automatically collect and store information about your use of the Website through certain cookies that are set. Please refer to our Cookies Policy, which is available on our website.

7. What obligations must Saint John of God Housing Association staff members comply with?

All Housing Association staff must keep confidential any personal data they are using as part of their employment. Not all staff members are expected to be experts in data protection law. However, The Housing Association is committed to ensuring that its staff are sufficiently aware of the data protection law in order to be able to anticipate and identify a data protection issue, should one arise.

The Housing Association has provided data protection awareness training to all staff members which provides staff with the ability to recognise, report and address potential data breaches and to respond to subject access requests efficiently. Staff have been trained to ensure that where personal data must be shared with suppliers that The Housing Association will only use suppliers who have robust data protection policies in place (See Third Party Processors below).

The Housing Association is obliged to keep personal data accurate and up to date. Any information which is incorrect or misleading and The Housing Association must take steps to check the accuracy of any personal data when it is being collected and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

Staff members should ensure that they notify the Planning and Development Manager / CEO of any relevant changes to their personal information so that it can be updated and maintained accurately, for example, a change of address.

Personal data should not be kept longer than is necessary. For guidance in relation to data retention staff members should contact the Planning and Development Manager / CEO. The Housing Association has various legal obligations to keep certain employee data for a specified period of time. **The Housing Association will conduct regular assessments in order to establish the need to keep certain Personal Data.** Where it is no longer required to be kept The Housing Association will destroy, erase or otherwise put this data beyond use.

8. How can staff members ensure that data is kept safe?

Staff members must ensure that data is kept safe by:

- a. Ensuring desks and cupboards are kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.) Please refer to the Clear Desk Policy.
- b. When destroying information paper documents should be shredded. Floppy disks and CD-ROMs should be physically destroyed when they are no longer required.
- c. Data users should ensure that individual monitors do not show confidential information to passers-by and that they lock or log off from their PC when it is left unattended.
- d. Responsibilities

Everyone who works for or with The Housing Association has a responsibility for ensuring data is collected, stored and handled appropriately.

Each department that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, there are a number of key responsibilities:

- 1.1. The Board and Chief Executive of The Housing Association have the responsibility for ensuring that The Housing Association meets its legal Data Protection obligations.
- 1.2. The Data Protection Officer/ Planning and Development Manager is responsible for:
 - ✘ Keeping the Chief Executive and the Board updated about data protection responsibilities, risks and issues;
 - ✘ Informing and advising the Company and the employees of their obligations under the Regulation;
 - ✘ Monitoring compliance with the Regulation and with Company policies in relation to the protection of personal data, including managing internal data protection activities, training staff and conducting internal audits;
 - ✘ Providing advice, where requested, concerning the Data Protection Impact Assessments (DPIA) and monitor its performance; cooperate with the supervisory authority; and act as the point of contact for the supervisory authority on issues relating to processing and with regard to any other matter;
 - ✘ In addition, the Data Protection Officer (DPO) is required to have due regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.
 - ✘ Dealing with requests from individuals to see the data that The Housing Association holds about them (also called: "subject access requests"); and,
 - ✘ Checking and approving any contracts or agreements with third parties that may handle the Company's sensitive data.

General staff guidelines:

- ✘ The only people able to access data covered by this policy should be those who need it for their work.
- ✘ Data should not be shared informally. When access to confidential information is required, employees can request it from their line manager.
- ✘ The Housing Association will provide training to all employees to help them understand their responsibilities when handling data.
- ✘ Employees should keep all data secure, by taking sensible precautions and following the guidelines.
- ✘ In particular, strong passwords must be used and they should never be shared.
- ✘ Personal data should not be disclosed to unauthorised people, either within the organisation or externally.
- ✘ Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of in accordance with our retention policy.
- ✘ Employees should request help from their line managers or the Data protection Officer if they are unsure about any aspect of data protection.
- ✘

e. (e) Refer to the ICT Security Policy.

9. Providing Information over the telephone

Any staff member dealing with telephone enquiries should be careful about disclosing any personal data held by The Housing Association over the phone. In particular the employee should:

- a. Check the identity of the caller to ensure sure that information is only given to a person who is entitled to that information.
- b. Suggest that the caller put their request in writing if the staff member is not sure about the identity of the caller and in circumstances where the identity of the caller cannot be verified.
- c. Refer the request to their manager for assistance in difficult situations. No staff member should feel forced into disclosing personal information.

10. How does Saint John of God Housing Association manage personal data queries?

Under data protection law personal data must be acquired and managed fairly. The Housing Association will manage all requests through the Director of ICT at HMQ in the interim until the role of the Data Protection Officer is filled. They are responsible for monitoring and continually improving our internal data protection processes. *(DPO Position under recruitment at 25th May 2018).*

11. Subject Access Requests

If a data subject requests a copy of their personal data, this is known as a Subject Access Request. The request does not have to be in writing. However, the request must be accompanied by required proof of identity and address. All requests will be processed in a timely manner and within not more than 30 days from the receipt of the request or in accordance with the legislation. For ease of convenience, we have created a Subject Access Request form to assist data subjects in making a request. It can be a useful checklist as to what information is required from the data subject when making a request. A copy of the Subject Data Request form is available on request.

12. Third Party Processors

As The Housing Association controls, and is responsible for keeping and using, personal data on its computers or in manual files, it is known as a Data Controller. This means The Housing Association has obligations under the legislation to keep the data safe. As part of its day-to-day business activities, The Housing Association engages third parties to carry out work on its behalf. Some of these third parties must hold or process the personal data to perform their job. These third parties are known as Data Processors. To ensure that all personal data that is held or processed by Data Processors is kept safe, a written agreement is entered into with the Data Processor, which sets out their obligations to The Housing Association. It sets out the specific purpose or purposes for which they are engaged, on the understanding that they will process the personal data in compliance with Data Protection legislation.

13. Data Breaches

It is important that all staff are aware to whom they should report such a breach. Staff need to be made fully aware as to what constitutes a breach. The Housing Association has a data breach policy in place and this forms part of staff awareness training.

Having such a procedure in place will allow staff to recognise a breach or a potential breach early on so that it can be dealt with in the most appropriate manner

The Housing Association is required under the GDPR to report certain types of personal data breach to the Data Protection Commission (DPC) within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, The Housing Association must also inform those individuals without undue delay.

14. Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data in manual or electronic form. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal Data Breaches may include:

- ✘ access by an unauthorised third party;
- ✘ deliberate or accidental action (or inaction) by a controller or processor;
- ✘ sending personal data to an incorrect recipient through email, fax etc;
- ✘ computing devices containing personal data being lost or stolen;
- ✘ alteration of personal data without permission; and loss of availability of personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. Therefore, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed. In accordance with Recital 87 of the GDPR when a security incident takes place, it must be quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including informing the Data Protection Commissioner.

The risk of having a data breach can be greatly reduced/minimised by adherence to SJOG Ministries Corporate ICT security policies (under review), ensuring the security of manual personal data and maintaining a clear desk policy.

What happens if a breach occurs?

Actual, suspected, or potential breaches need to be reported immediately to your line manager whom will report it to the person / entity acting as Data Protection Officer (DPO).

Any employee who becomes aware of a likely data breach and fails to follow the procedure may be subject to The Housing Association's disciplinary procedures.

On receipt of the notification a team comprising the DPO and other relevant staff will be established to assess the breach and determine its severity. Depending on the scale and sensitivity of data lost and the number of Data Subjects impacted, the Office of the Data Protection Commissioner and relevant regulatory bodies will be informed as quickly as possible following detection. If a breach is considered likely to result in a high risk to the rights and freedoms of individuals, The Housing Association will inform the individuals concerned directly and without undue delay and provide them with an assessment of the risk to their privacy. The Housing Association will make recommendations to the data subjects which may minimise the risks to them. The Housing Association will then implement changes to procedures, technologies or applications to prevent a recurrence of the breach.

When will the Office of the Data Protection Commissioner be informed?

All incidents in which personal data has been put at risk will be reported to the Office of the Data Protection Commissioner. The only exceptions to this policy are when the data subjects have already been informed, where the loss affects fewer than 100 data subjects, and where the loss involves only non-sensitive, non-financial personal data.

Where devices or equipment containing personal or sensitive personal data are lost or stolen, the Data Protection Commissioner is notified only where the data on such devices is not encrypted.

15. Data Loss Incident Logging

All data breaches will be recorded centrally in an incident log by the The Housing Association. The log will maintain a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and an explanation of why the Office of the Data Protection Commissioner was not informed. Such records will be provided to the Office of the Data Protection Commissioner upon request. This incident report must be completed immediately by The Housing Association employees and their line manager whenever confidential or personal data belonging to The Housing Association is accidentally disclosed, lost or stolen, or whenever a Housing Association mobile computer device or a mobile storage device is lost or stolen.

The completed report must be forwarded immediately via fax or email (a scanned copy) to the person / entity responsible for the role of Data Protection Officer. The Data Protection Officer will liaise with relevant personnel to ensure the correct course of action is taken.

16. Enforcement

The Policy applies to all employees of The Housing Association. It also applies to contractors and temporary personnel of The Housing Association

Adherence to the Policy is overseen by line management. If an employee considers that the Policy has not been followed in respect of personal data about themselves or others they should raise the matter with their line manager as soon as possible.

The Planning and Development Manager will monitor any breaches of the Policy and will work in tandem with line management to ensure ongoing general compliance. Data protection training is mandatory for all employees and training will be continually offered for employees.

Any breach of the Policy will be taken seriously and depending on the severity and nature of the breach may result in disciplinary action up to and including

dismissal. The Housing Association reserves the right to take such action as it deems appropriate against any data users who breach the conditions of this policy.

17. Review of Policy

The Housing Association will continue to review the effectiveness of the Policy to ensure it is achieving its stated objectives on at least an annual basis and more frequently if required taking into account changes in the law and organisational or security changes.

Next Review Date: 26th May 2020.

18. References

For further information relating to data protection please refer to:

- ✘ Saint John of God Housing Association's Subject Access Request Form
- ✘ Saint John of God Housing Association's Website Privacy Statement
- ✘ Data Protection Commissioner's Website <https://www.dataprotection.ie>

Disclaimer: This publication is for guidance purposes only. It does not constitute legal or professional advice. No liability is accepted by Saint John of God Housing Association clg for any action taken or not taken in reliance on the information set out in this publication. Professional or legal advice should be obtained before taking or refraining from any action as a result of the contents of this publication. Any and all information is subject to change.

Saint John of God Housing Association CLG
Gleann na hEorna
Tessa House, Block D
Springfield
Tallaght
Dublin 24

Telephone: 01-468 6452
Email: housing@sjog.ie