



Hygiene Hub

Hygiene Hub Data Protection Policy

Introduction

Hygiene Hub Company Limited by Guarantee (“Hygiene Hub”) is a grass-roots, people-powered charity working to end hygiene poverty across Ireland by freely providing hygiene, personal care and household cleaning items to those who need them. We are compassionate, collaborative and rooted in community. We believe that being clean is a right, not a privilege and yet many in Ireland cannot afford the everyday essential hygiene items most of us take for granted. We are a network of supporters, volunteers and partners working towards a simple mission: to tackle hygiene poverty across Ireland.

Purpose

The purpose of this policy is to set out the procedures for keeping sensitive data secure to avoid data breaches. It also sets out the procedure for dealing with deleting sensitive data and dealing with a data breach.

Scope

This policy applies to all volunteers, employees and trustees of Hygiene Hub, as well as members of the public who interact with Hygiene Hub or its services.

When Hygiene Hub collects sensitive data

Hygiene Hub collects data when:

- A supporter donates online via platforms such as iDonate
- A supporter signs up to the newsletter
- A supporter signs up to volunteer
- A member of the public contacts Hygiene Hub
- A Community Partner agrees to be supported by Hygiene Hub

- A local business, school or college agrees to host a Drop Off Point or run a short term collection, or makes a donation of hygiene items
- A business or corporate entity agrees to support Hygiene Hub

As a supporter

If you are providing us with your personal data through joining our newsletters (for example, your email) we will keep your data until you request its deletion.

If you are providing us with personal data in relation to being a Corporate Partner, Community Partner, Schools Partner (for example; email or phone number) we will keep this data until support is withdrawn or you request its deletion.

If you are providing us with your personal data as a financial donor, we will keep your data for as long as you continue to give us your financial support and as required to operate our services in accordance with legal, tax and accounting requirements. This will be a period of not longer than 7 years. Where your information is no longer required, we will ensure it is disposed of in a secure manner. Where a donor joins any newsletter, their contact information will be retained purely for that purpose.

What data is collected?

Fundraising or donating online - Supporters opt in to giving us their contact details (full name, address, email, phone number). They can also opt in to receiving our newsletter. This information is saved on Google Drive and Salesforce.

Supporters can request to receive an automatic receipt of donation from iDonate. Where significant funds have been donated, a supporter might be contacted with a formal receipt of donation and thank you note.

iDonate collects sensitive data as part of the payment process. iDonate holds sensitive data in relation to donations for 3-6 months, depending on the donation type. More information can be found here: <https://www.idonate.ie/privacy-policy/>

Newsletter - When supporters opt in to be sent our newsletter, we collect their name and email address. Supporters will be contacted by email with a newsletter at regular intervals (e.g. monthly or quarterly).

This information is saved on Wix and Brevo servers in compliance with GDPR.

Volunteering - New volunteers provide their contact details (full name, address, email, phone number). Volunteers are contacted via email and phone, predominantly Whatsapp.

This information is saved on Salesforce, Google Drive and Whatsapp. Where contact is relevant and necessary, a volunteer's mobile number may be saved by other volunteers on their phones.

Community Partners - Community Partners provide details of their organisation (name and address) and provide contact details for main contact at the organisation (full name, email address, phone number). Contact might be via email or phone. This information is saved on Google Drive and Salesforce.

Where contact is relevant and necessary, the contact details of individuals in Community Partners may be saved by Hygiene Hub volunteers on their personal phones.

Local businesses - Local businesses provide details of their organisation (name and address) and provide contact details for main contact at the organisation (full name, email address, phone number). Contact might be via email or phone. This information is saved on Google Drive and Salesforce. Where contact is relevant and necessary, the contact details of individuals in local businesses may be saved by Hygiene Hub volunteers on their personal phones.

Corporate partners - Partners provide details of their organisation (name and address) and provide contact details for main contact at the organisation (full name, email address, phone number). Contact might be via email or phone.

This information is saved on Google Drive and Salesforce.

Ambassadors - Ambassadors provide personal details (name, email, phone number, county), as well as their background and any relevant experience. Contact might be via email or phone.

This information is saved on Google Drive and Salesforce.

Storing sensitive data securely

Sensitive data must be correct, safe, and stored securely. This means:

- That only the people who are authorised to use the data can access it. Documents with sensitive data are password protected or saved in sensitive folders with limited access. Hub Coordinators should hold and maintain sensitive data relating only to their local hub and sensitive data relating to Hygiene Hub's national work should be maintained only by the Head Office Team.
- That the data is accurate and kept up to date when contact details change. That mailing lists are kept up to date, taking into account those who have 'opted out'.

- That sensitive data is used only for the purposes as intended. If a stakeholder has not opted in to the newsletter, they should not receive it. Stakeholders should only be contacted with information that is relevant to the purpose of the partnership.
- That individuals have a right to access their own personal information held by Hygiene Hub.

How Hygiene Hub might use sensitive or personal data

The legal reason for processing data will depend upon the circumstances in which it is being collected and used, but will in most cases fall into one of the following categories:

- Where a supporter has provided consent to allow us to use data in a certain way (e.g. if you have opted to receive regular updates about our work).
- Where the processing is necessary to carry out a contractual relationship (e.g. as a referral agent, a client in receipt of our services or a contractor carrying out work on our behalf).
- Where the processing is necessary in order for us to comply with a legal obligation (e.g. when a supporter signs up as an official volunteer).
- Where it is in Hygiene Hub's legitimate interests to perform our functions (e.g. processing donations or sending administrative communications where our legitimate interest is to deliver our charitable purposes).

Examples include:

- When a supporter has given consent to receive the Hygiene Hub newsletter
- When a supporter has donated and requires a receipt
- When a supporter has signed up to fundraise
- When a supporter has signed up to volunteer

Sharing sensitive information

- Hygiene Hub must never sell any personal information to any organisation for any reason.
- Hygiene Hub must not pass personal data on to any other country or international organisation unless explicitly outlined in this policy.
- Hygiene Hub will not use personal data in any automated decision-making or automated profiling activities.

Hygiene Hub may share data with another party with consent for one or more of the following purposes:

- Companies directly connected to Hygiene Hub, such as Community Partners, Brand Partners, or couriers.
- Irish Revenue – to make claims on tax back.
- Banks or other payment providers – to authorise or make transactions.
- Financial and legal advisers in the event we need to obtain advice and protect or defend our legal rights.

Hygiene Hub may need to share data with law enforcement bodies in order to comply with any legal obligation or court order. Hygiene Hub will not share personal data without notifying the relevant person.

Deleting sensitive data

Hygiene Hub will store sensitive data for the period of time that the supporter, volunteer or partner gives their time and support. For information around financial support that is required to operate Hygiene Hub's services in accordance with legal, tax and accounting requirements, this is 7 years. This section outlines the process when Hygiene Hub might need to delete sensitive data.

When contacts in partnership organisations change

When a point of contact changes for an organisation (whether a corporate partner who supports Hygiene Hub or a Community Partner who is supported by Hygiene Hub) Hygiene Hub should delete the contact information of the old contact and this should be immediately replaced with contact information for the new contact. Community Partner or Corporate Partner contact details should be updated as well as any mailing lists where the contact details are present.

When a volunteer stops volunteering

When a person stops volunteering, the contact details will be removed from volunteer mailing lists, Whatsapp groups and phone contacts. Consent to add their contact details to the Supporter's mailing list will be requested from the person ceasing volunteering. The volunteer will be removed from mailing lists and Whatsapp groups no later than 30 days after they step back.

Completion of this process should be verified by the head office team.

Hygiene Hub will retain a volunteers' personal information for 2 years after someone has stopped volunteering, unless for specific purposes (for example; if they have signed up to the Supporter Newsletter). A volunteer may request their personal data be deleted upon stopping volunteering.

The volunteer who is stepping back must delete any sensitive documents that relate to Hygiene Hub. The volunteer will sign to confirm that all sensitive information is deleted.

When a supporter or partner exercises their right to be forgotten

When asking to be forgotten, Hygiene Hub should agree to the request unless their data is needed to uphold the right to the freedom of expression, it is needed for legal obligations, or it is needed for reasons of public interest. Hygiene Hub should carry out the request within 30 days of it being received. This request will be actioned by the IT team at Hygiene Hub and its confirmed by the Data Protection Officer.

Subject Access Requests

Past or present supporters, volunteers, employees and partners or any others have the right to request a Subject Access Request. This might be to view or correct information Hygiene Hub currently holds. Hygiene Hub will comply with the Subject Access Request and should respond within 30 days of the request. Following a Subject Access Request, a supporter, volunteer or partner can exercise their right to be forgotten. Hygiene Hub should agree to the request within 30 days of it being received.

Breaches in data protection

A data breach refers to a breach of security that leads to the destruction, loss, alteration, unauthorised access to, or unauthorised disclosure of personal data. This section outlines how to deal with a data breach.

1. Contact the designated Hygiene Hub Data Protection Officer. The incident must be recorded in the incident register and the impact assessed.
2. The incident register will be presented to the Board at the next Board meeting, or earlier if required.
3. The relevant supervisory authority should be alerted. This may include the Data Protection Commission. The individual should also be alerted. This should take place within 72 hours of the breach being realised.
4. The DPO should take advice from the Commission on the next steps.

Designated Data Protection Officer: Liz Burrows

All volunteers should contact **Liz Burrows** for any concerns/queries they have in regards to data protection or data breach. Hygiene Hub should be transparent and accountable in responding to concerns. A log of the issue must be kept on the Incident Register.

Contact via: info@hygienehub.ie

Revision history and next review

Policy Document:	Data Protection Policy
Date of Next Review	September 2028
Version:	3.0
Approved by, Date:	
Last Reviewed:	September 2025

Signed:

DocuSigned by:

 B0D85557725C49A...

Chair of the Board