

Helium Arts

Data Privacy Policy

Document Creation and Review History			
Date:	Reviewed by:	Document amended:	Next date for review
May 2018		Created by Anna McCarthy, approved by the Board in 2018	2020
November 19, 2021	Mason Hayes and Curran	Updated	
November 2021	Governance Committee / James Quaine	Governance Committee > James Quaine > Mason Hayes and Curran > Helene Hugel	
December 2021	Board	Approved by the board on Wednesday, December 22, 2021	December 2023
Oct 2024		Reviewed by Walkers with Helium Arts	
28 November 2024	Governance Committee / James Quaine	Governance Committee > James Quaine > Mitzi D'Alton	
18 December 2024	Board	Approved by the board on 18 December 2024	February 2026

1. SCOPE OF POLICY

This Policy relates to the collection and Processing of Personal Data by Helium Arts "Helium" in the course of its activities.

Helium makes no distinction between the rights of different Data Subjects. All Data Subjects whose Personal Data are Processed by Helium are treated equally under this Policy.

The Policy applies equally to Personal Data held in manual and automated form.

To the extent that there are inconsistencies between this Policy and Relevant Legislation, then the Relevant Legislation shall prevail and this Policy shall be construed accordingly.

2. DEFINITIONS

For the avoidance of doubt, and for consistency in terminology, the following definitions will apply in this Policy.

Term	Meaning
"Controller"	the organisation which determines the purposes and means of the Processing of Personal Data.
"Data"	this includes both automated and manual data. Automated data means data held on computer, or stored with the intention that it is Processed on a computer. Manual data means data that is Processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.
"Data Subject"	a living individual who is the subject of the Personal Data, i.e. to whom the data relates either directly or indirectly.
"GDPR"	General Data Protection Regulation (Regulation (EU) 2016/679)
"Personal Data"	any information relating to an individual who can be identified, directly or indirectly from such data, including, for example, such individual's name, residential address, email address and financial details. Descriptions of individuals with sufficient specificity will also be considered Personal Data.
"Policy"	this Data Protection Policy.
"Processing"	any use of Personal Data, including, for example, storage in databases, input onto systems and sharing with third parties. "Process", "Processed", "Processing" and "Processes" shall be construed in accordance with the definition of "Processing".

"Processor"	any organisation(s) Processing Personal Data on behalf of the Controller.
"Relevant Legislation"	the Data Protection Acts 1988 to 2018 and the GDPR.
"Special Categories of Personal Data"	sensitive Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data and biometric data, data concerning health or data concerning an individual's sex life or sexual orientation.

3. IMPLEMENTATION AND ENFORCEMENT OF POLICY

Helium will ensure that adequate steps are taken to maintain compliance with this Policy. This includes:

- (a) designating Mitzi D'Alton to act as a Data Protection Officer (see section 4 below);
- (b) conducting an annual review of the Policy to ensure that it provides an accurate description of Helium's data protection framework;
- (c) receiving annual reporting on and/or conducting an annual review of the data protection policies and procedures of Processors to ensure ongoing compliance with service standards; and
- (d) ensuring that Helium's employees and members of the board of directors of Helium the "**Representatives**" receive data protection training and are informed of Helium's responsibilities in respect of this Policy.

Where any material non-compliance with the Policy is identified, remediation measures will be implemented.

4. DATA PROTECTION OFFICER

Helium has designated a data protection officer for the purposes of compliance with Article 37 of the GDPR on the basis that Helium's core activities consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Helium has appointed Mitzi D'Alton to fulfil the role of Data Protection Officer. The Data Protection Officer is responsible for:

- (a) co-operating, as necessary, with the Irish Data Protection Commission "**DPC**" in respect of Helium's compliance with the Relevant Legislation;
- (b) conducting an annual review of the Policy to ensure that it is line with Relevant Legislation and provides an accurate description of Helium's data protection framework;
- (c) ensuring that Processors provide an annual report and/or facilitate an annual review to ensure compliance with service standards;
- (d) monitoring compliance with Relevant Legislation;

- (e) acting as a point of contact for individuals whose Personal Data are Processed by Helium; [contact via info@helium.ie](mailto:info@helium.ie) or 044 939 6960
- (f) reporting directly to the board of directors of Helium on data protection related matters; and
- (g) ensuring that Helium maintains a record of all of its Personal Data Processing activities.

5. DATA PROTECTION STATEMENT

Helium is committed to privacy and respecting the rights of those whose Personal Data we collect and use in accordance with applicable law.

Data protection is about providing individuals with protection as to how information about them is used by organisations. This protection is enshrined in the Relevant Legislation.

To provide this protection, data protection law establishes good data handling and data management principles. It also grants specific rights to individuals regarding their Personal Data which is Processed by Helium. Helium is committed to respecting and supporting the right to data protection, including the rights of individuals under applicable law to control the dissemination and use of the Personal Data that relates to them.

6. DATA PROCESSING BY HELIUM

In the course of its daily organisational activities, Helium acquires, Processes and stores Personal Data in relation to:

- (a) the parent/guardian registering with Helium on behalf of a child;
- (b) the child using Helium's services;
- (c) medical practitioners (incl. GP, consultants, social/care workers;
- (d) Employees; and
- (e) Prospective employees.

The categories of Personal Data can be summarised as follows:

- (a) **Parent/Guardian:** In respect of the parent/guardian registering with Helium for Helium services on behalf of a child, Helium collects the following personal data: name, email address and telephone number, emergency contact information and GP name.
- (b) **Child registered with Helium:** In respect of the child being registered for Helium services, Helium collects the following personal data: name, date of birth, gender, data relating to the child's health, allergy information, GP name, name of child's consultant or key health/social care worker (in order to verify their eligibility). Data relating to health is considered Special Categories of Personal Data under EU data protection law and therefore this data is subject to additional safeguards and protections. To the extent that Helium Processes any Special Categories of Personal Data, Helium does so on the basis of exercising our duty of care

towards children using our services and necessity for defence of any legal claims which may arise.

- (c) **Third Party Volunteers and Healthcare Workers etc.:** In respect of healthcare workers, social, community & youth workers or teachers referring a child to Helium services on behalf of a child, Helium collects the following personal data: name, title, email address and telephone number.
- (d) **Donors & Sponsors:** In respect of the donor / sponsor's support of Helium services, Helium collects the following personal data: names, contact details and (where relevant) their payment information for the purposes of performing the contract entered into with them, such as for sponsorship, donation purposes.
- (e) **Volunteers:** In respect of the volunteer's support of Helium services, Helium collects the following personal data: names, contact details and photo ID and proof of address for vetting for the purposes of performing the contract entered into with them, such as for volunteer purposes.

Personal Data are Processed and transferred for the following core purposes:

- (a) For the purposes of performing contracts entered into by Helium. Where Helium needs to perform a contract it is about to enter into or has entered into with a third party, Helium relies on contractual necessity for the Processing of Personal Data related to those contracts. These contracts include:
 - (i) Contracts with parents/guardians: Helium Processes Personal Data for the purposes of performing the contracts it enters into with parents/guardians for the provision of Helium services. Helium process the parent's/guardian's name, email address and telephone number for the purpose of providing the Helium services.
 - (ii) Contracts with sponsors, donors and volunteers: Helium Processes Personal Data for the purposes of performing the contracts it enters into with sponsors, donors and volunteers. Helium Processes those individuals' names, contact details and (where relevant) their payment information for the purposes of performing the contract entered into with them, such as for sponsorship, donation and/or volunteer purposes.
- (b) Compliance with legal obligations: Helium Processes Personal Data in order to comply with its legal obligations, in particular Helium's Health and Safety obligations in respect of the children to whom it provides Helium services.
- (c) We Process Personal Data where required in line with our legitimate interests: Helium Processes Personal Data collected by Helium's website for website analytics purposes only (to help it gather and analyse information about the areas visited on the website in order to evaluate and improve the user experience and the website), unless a Data Subject gives Helium consent for their information to be used in other specific ways. Helium uses Personal Data in this way on the basis of its legitimate interests in operating an efficient website tailored to our users.
- (d) Helium Processes Personal Data for the specific purposes for which a Data Subject provided their consent: These purposes might include

circumstances where a Data Subject provides their email address and information about themselves or their organisation so that Helium can contact them, so that they can donate to Helium, so that they can register for an event, and / or so that Helium can provide them with updates about our work and events.

- (e) Helium Processes Personal Data for the purposes of corresponding with its supporters: Helium stores the contact information of donors, supporters and sponsors who have consented to give their information, in order to send correspondence containing information relevant to the work supported.
- (f) Helium Processes Personal Data for marketing purposes on the basis of your express consent: Where a data subject has specifically consented to our use of their personal data, for example to send direct marketing communications to them via email, Helium will process their Personal Data for those specific purposes. In those circumstances, a Data Subject has the right to withdraw their consent to marketing at any time by unsubscribing from our newsletter or contacting Helium.

Children's Personal Data

As many of the beneficiaries of Helium's work are under the age of 18, Helium acknowledges that they are all below the legal age for giving consent to the Processing of their Personal Data. All of our data collection and Processing activity therefore is undertaken in the understanding that it will be directed and responded to by the parent/guardian in the children's life that will be using it. Any Personal Data that Helium requests about the children who take part in our activities - including taking pictures and video - will always be gathered with the express consent of the parent or guardian.

Pictures and Video of Children

"The use of images play an important role in many aspects of work with children and young people. Images in many formats can be used to record, document, demonstrate, promote and celebrate activities and experiences. Increasingly, accessible and diverse technology has meant that recording, sharing, disseminating and publicising images is more widespread than ever before." (Source: The Arts Council, 'Guidelines for taking and using images of children and young people in the arts sector')

Helium has a clear policy in place for capturing images of children for documentation, archiving or promotional use:

- Images can only be captured with the written consent of the child's parent or legal guardian. Other adult relatives are unable to give consent for this.
- Withholding of consent must never affect or limit the child's experience of the activity they are taking part in.
- Even if a parent has given consent, if a child decides that they don't want their picture taken, their wishes must be respected.
- Parents taking pictures of their own child at a Helium project is acceptable (assuming it's not disruptive to the event or infringing artists' copyright) but if they're taking pictures that include other children, they should be reminded of the importance of data protection and ask them to refrain from taking pictures featuring other children. If that is unavoidable, they should be reminded that these images should not be shared online.
- Capture of images should be done in a respectful way, with no or

- minimal impact on the focus or experience of the children.
- Care must be taken to avoid inadvertent discrimination or stereotyping of any child, particularly on the basis of disability, ethnicity or gender.
- Images should not include Personal Data such as name badges or school crests. Where they do appear, they should be removed or obscured using editing software.
- Accompanying photo credits should be mindful of giving information that could be used in a way that threatens the child's safety - eg their name or specific address details.
- Images of children's artwork should only be taken with the permission of the child and any names should be cropped out.
- Images featuring unidentifiable aspects such as a child's hands, silhouette or the back of their head can be captured but it must be impossible to identify or recognise the child based on that photograph.

Duration of Use

Despite consent being given for the indefinite use of images, in line with Helium's commitment to the protection of children Helium has decided to put a period of five years on retention for promotional use. This will avoid potential embarrassment for children of their imagery being used when they are significantly older. It also ensures that Helium will have ceased using their image for promotional use before they turn 18. After 5 years, images will only be used for archival and reporting purposes.

2. DATA PROTECTION PRINCIPLES

The data protection principles stipulated below set out the main responsibilities which apply to Helium when Processing Personal Data. Whenever Helium Processes Personal Data, it should comply with these data protection principles.

Fairness/Transparency: Helium should only use Personal Data in a fair, lawful and transparent manner:

- (a) whenever Helium collects Personal Data from Data Subjects, the Personal Data should only be Processed when the relevant Data Subject has been presented with a privacy notice at the point of collecting their Personal Data; or
- (b) whenever Helium obtains Personal Data relating to a Data Subject otherwise than directly from the Data Subject, Helium should provide the Data Subject with a privacy notice containing the information stated in Article 14 of the GDPR:
 - (i) within a reasonable period after obtaining the Personal Data, but at the latest within one month, having regard to the specific circumstances in which the Personal Data are Processed;
 - (ii) if the Personal Data are to be used for communication with the Data Subject at the latest at the time of the first communication to that Data Subject; or
 - (iii) if a disclosure of the Personal Data to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

- (c) the privacy notice should set out clearly and in plain language the categories of Personal Data being collected and the way in which Helium will Process this Data. The contents of privacy notices must meet the requirements of Relevant Legislation; and
- (d) any new data Processing initiatives which are likely to result in a high risk to individuals' interests must be subject to a privacy impact assessment and new approved initiatives may require the adoption of a new privacy notice which outlines the way in which Helium will Process Personal Data (if current privacy notices are not adequate).

Purpose Limitation: Helium should only Process Personal Data for specific stated purposes:

- (a) Personal Data should only be Processed in line with the purposes set out in the privacy notice;
- (b) if sharing Personal Data, Helium should ensure it is only shared with those who require access to achieve the stated purposes;
- (c) Processing Personal Data for purposes other than those set out in the relevant privacy notice is subject to approval and sign-off from the board of directors of Helium.

Data Minimisation: Helium should only collect and Process Personal Data which is necessary for achieving the purposes set out in the privacy notice. If a specific category of Personal Data does not serve a purpose, it should not be collected.

Accuracy: Helium should ensure Personal Data are accurate and up-to-date:

- (a) it is essential that the Personal Data Helium holds remains up-to-date and accurate;
- (b) when Personal Data are inaccurate, it should be corrected (particularly if an individual makes a request to correct their Personal Data); and
- (c) Personal Data which is out of date should be updated or deleted.

Storage Limitation: Helium should only retain Personal Data for as long as is necessary:

- (a) Personal Data should be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the Personal Data are collected and Processed; and
- (b) if there is value in retaining Personal Data in some form for prolonged periods of time, it should be considered whether it is possible to derive a benefit from the data without the Personal Data. If the Personal Data can be anonymised or pseudonymised, this should be done.

Integrity and Confidentiality: Helium shall keep Personal Data secure:

- (a) Personal Data must be stored and Processed in a secure manner;
- (b) in practice, Personal Data should not be shared with anyone who does not require access to the Personal Data;

- (c) where possible and appropriate, Personal Data should be password protected and/or encrypted before sharing it with anyone (internally or externally), particularly if the sharing is via email. Good security practices should be adopted, such as using robust passwords and encrypting hardware; and
- (d) if it is possible, Personal Data should be stored in a pseudonymised / de-identified form.

Data Transfers: International transfers of Personal Data:

- (a) all transfers of personal data outside of the EEA are subject to the approval of the board of directors of Helium and shall only be permitted where they are in accordance with the privacy notice or are otherwise permitted by Relevant Legislation; and
- (b) Helium will ensure that a suitable transfer solution is in place to safeguard the Personal Data being transferred (for example, by using model contract clauses).

Vendor Control: Engaging with third parties:

- (a) Third parties involved in the Processing of Personal Data on behalf of Helium must be subject to a contract which contains the required Personal Data protection terms; and
- (b) all agreements with third parties Processing Personal Data on behalf of Helium shall be subject to the approval of the board of directors of Helium.

2. LEGAL BASIS FOR PROCESSING

When Helium Processes Personal Data, it shall do so on the basis of one of the lawful grounds set out in the GDPR. The legal basis for each Personal Data Processing activity carried out by Helium must be detailed in privacy notices. Legal bases include: consent, performance of a contract, compliance with legal obligations and legitimate interests.

Whenever Helium Processes Personal Data it shall be clear which legal basis is being relied on. Helium's current practices have been assessed and the relevant legal bases are set out in the privacy notices.

In practice, for all new material Personal Data Processing activities, Helium should take the following steps:

- (a) identify the categories of Personal Data to be collected;
- (b) identify the purposes of Processing this Personal Data;
- (c) assess whether the current privacy notices are adequate;
- (d) if the current privacy notices are not adequate, new / updated privacy notices shall be prepared prior to collection of the Personal Data; and
- (e) where necessary, implement new technical solutions. For example, if relying on consent, implementing a consent mechanism.

3. INDIVIDUAL RIGHTS

Relevant Legislation provides a number of rights for individuals regarding their Personal Data which is being Processed by Controllers such as Helium. Helium shall respond to requests as soon as possible and subject to the deadlines set out under the Relevant Legislation.

Individuals have the right to make the following types of request regarding the Personal Data Helium holds about them:

- (a) Right to be informed – the Data Subject's right to be informed about whether their Personal Data is being Processed and their rights in relation to their Personal Data.
- (b) Right of access (subject access requests) – the right to request a copy of the Personal Data Helium holds concerning an individual and supporting information explaining how the Personal Data are used.
- (c) Right of rectification – the right to request Helium to rectify inaccurate Personal Data concerning an individual.
- (d) Right of erasure (right to be forgotten) – the right to request Helium erase all Personal Data concerning an individual.
- (e) Right to restrict Processing – the right to, in some situations, request Helium not to use an individual's Personal Data they have provided (e.g. if they believe it to be inaccurate).
- (f) Right to object – the right to object to certain Processing of his/her Personal Data (unless Helium has an overriding compelling legitimate grounds to continue Processing) and the right to object to direct marketing.
- (g) Rights relating to automated decision making – the right to object/opt-out of automated decision making that significantly affects an individual.
- (h) Right to data portability – the right to, in some situations, request Helium to port an individual's Personal Data to the individual or a new Controller in machine readable format.
- (i) Right to complain – the right to lodge a complaint about the way Helium handles or Processes the individual's Personal Data with the individual's national data protection regulatory authority.
- (j) Right to withdraw consent – If an individual has given consent to anything Helium does with their Personal Data, that individual has the right to withdraw their consent at any time. This includes the individual's right to withdraw consent to Helium using their Personal Data for marketing purposes. Any Processing of the Data Subject's Personal Data on the basis of their consent, up to the point at which the Data Subject withdraws their consent, is not unlawful.

In certain circumstances, Helium will be exempted from responding to certain requests. Helium may use these exemptions to the extent appropriate.

A request which does, or which may, concern Personal Data, should be notified to the Data Protection Officer [via email info@helium.ie](mailto:info@helium.ie) or phone 044 939 6960

Helium will usually not charge a fee for acting on requests by Data Subjects to exercise their rights under the Relevant Legislation. However, Helium may charge a reasonable fee to cover administrative costs of providing the information for:

- (a) baseless or excessive/repeated requests, or
- (b) further copies of the same information.

Alternatively, Helium may be entitled to refuse to act on the request.

Helium is generally obliged to respond to requests from Data Subjects to exercise their rights within one month from when the request is received but, if the request is going to take longer to deal with, Helium will inform the Data Subjects accordingly.

2. SECURITY

Relevant Legislation requires that Helium implements appropriate technical and organisational measures to ensure Personal Data are subject to a level of security appropriate to the risk associated with the Processing. Helium shall ensure that its delegates and service providers take appropriate technical and organisational measures with a view to protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing (including taking reasonable steps to ensure the reliability of employees who have access to the Personal Data).

3. INCIDENT RESPONSE

The response to any breach of Personal Data can have a serious impact on Helium's reputation and the extent to which the public perceives Helium as trustworthy. The consequential impact can be immeasurable.

Not all Personal Data protection incidents result in data breaches, and not all data breaches require notification. Therefore, exceptional care must be taken when responding to data breach incidents.

A breach is a loss of control, compromise, unauthorised disclosure, unauthorised acquisition, unauthorised access, or any similar term referring to situations where persons other than authorised users, for an authorised purpose, have access or potential access to Personal Data in usable form, whether manual or automated. This could mean:

- (a) loss of a laptop, memory stick or mobile device that contains Personal Data;
- (b) lack of a secure password on computers and applications;
- (c) emailing Personal Data to someone in error;
- (d) giving a system login to an unauthorised person; or
- (e) failure of a door lock or some other weakness in physical security which compromises Personal Data.

Actual, suspected, or potential breaches should be reported immediately to the Data Protection Officer.

All data breaches will be recorded by the Data Protection Officer in an incident log. 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 (if applicable) an explanation of why the relevant regulatory authority was not informed.

Requirement to Notify

- (a) Relevant Legislation imposes strict requirements to notify the DPC in the event of a data breach.
- (b) If a notifiable data breach occurs, Helium shall notify:
 - (i) the DPC without delay and not later than within 72 hours of becoming aware of the data breach; and
 - (ii) affected individuals, unless any of the following applies:
 - (A) Helium has implemented security measures to ensure the Personal Data are unintelligible to anyone not authorised to access it (e.g. the Personal Data are encrypted);
 - (B) Helium has taken measures to ensure the high risk to individuals is no longer likely to materialise; or
 - (C) notifying the individuals concerned would involve disproportionate effort. In this instance a public communication or similar would be provided for the individuals concerned to ensure that they are informed in an equally effective manner.

Incident Response Objectives

- (a) In the event of a data or cyber breach incident Helium's primary objectives are to:
 - (i) stop the incident and limit the damage caused;
 - (ii) prevent the spread/loss of data;
 - (iii) recover data and/or systems that have been lost/stolen/damaged or otherwise compromised;
 - (iv) minimise the impact of the incident on the business and get 'up and running' again as soon as possible;
 - (v) identify risks arising from the incident;
 - (vi) notify appropriate parties or authorities of the incident;
 - (vii) learn from the incident; and
 - (viii) take steps to prevent future incidents.

2. DATA RETENTION

Helium should only retain Personal Data for so long as is necessary in connection with the purposes for which it was collected.

3. DATA SHARING

Helium may share Personal Data with third parties. These third parties can be categorised broadly as follows:

- (a) **Service providers:** including those listed in Schedule 1 hereto;
- (b) **Non-contractual parties:** e.g. Government agencies and law enforcement agencies; and
- (c) **Other third parties as authorised by the individual.**

Certain Service Providers may act as Controllers in respect of Personal Data shared by Helium whereas other Service Providers may act as Processors. Helium will ensure that a formal written contract is in place with each Processor containing all of the mandatory contractual requirements under the Relevant Legislation.

4. PRIVACY NOTICES AND CONSENT

Subject to the information contained in Section 7.2 of this Policy, whenever Helium collects Personal Data from individuals we shall provide information regarding the following as part of a privacy notice:

- what Personal Data are being collected;
- why it is being collected;
- how it will be used;
- who will have access to it; and
- the rights individuals have in relation to their Personal Data.

If the Data Protection Officer considers it necessary to obtain the consent of individuals to collect and Process their Personal Data, a consent mechanism must be implemented.

5. DATA PROTECTION BY DESIGN AND BY DEFAULT

Relevant Legislation requires Helium to conduct a privacy impact assessment before carrying out Processing of Personal Data in particular circumstances. A privacy impact assessment is an assessment of the risks and mitigations involved in Processing Personal Data.

Relevant Legislation also requires Helium to have in place measures and processes which demonstrate that privacy has been factored into all new business processes, vendors, projects, products or services where relevant. This is known as "privacy by design" and "privacy by default".

In practice this means Helium shall conduct a privacy impact assessment in circumstances where any new data Processing initiatives are likely to result in a high risk to individuals' interests. This may include the collection of Personal Data through a new channel or the sharing of Personal Data with a new third party.

6. MARKETING

Helium shall not use Personal Data to send marketing information to any individual unless the individual has given consent to receive such marketing information or unless the marketing is otherwise permitted under Relevant Legislation i.e. based on the legitimate interests of Helium to conduct marketing.

If an individual requests Helium to stop Processing their Personal Data for direct marketing purposes, Helium shall stop Processing the Personal Data for those purposes in accordance with the deadlines specified by Relevant Legislation.

7. DATA PROTECTION TRAINING

Data protection training will be made available for Helium's Representatives. Helium maintains a record of the data protection training which has been delivered and who has received this.

8. CHANGES TO THIS POLICY

Helium reserves the right to change this Policy at any time. Material changes will be notified to affected parties as appropriate.

Last Approval Date: 18 December 2024

Schedule 1

Data Processor	Services Provided to Helium
• iDonate	Donation Processing
• Stripe	Donation Processing
• Paypal	
• Mailchimp	Manage mailing lists, e-newsletters, e-marketing campaigns and automations
• Eventbrite	Managing occasional event bookings
• WordPress	Website platform
• Google Services, including Workspace and YouTube	Intranet, word processing, team collaboration. YouTube: video content and sharing
• Google Forms	Service user sign-ups. Collection of user personal data.
• Survey Monkey	Stakeholder evaluation surveys. Collection of user personal data.
• Vimeo	Video content and sharing
• Padlet	Video & Image content and sharing
• Medcore	Medical services provider at workshops
• Hubspot	CRM system for volunteers, staff, donors/funders, and stakeholders.
• Freenow	Taxi application used to provide transport to families.