GDPR Privacy and Data Protection Policy

Policy details

Policy became operational on:	May 25th 2018
Next review date:	December 1st 2018
Data protection registration number	ZAI82288 (HCI -charity)

Introduction

Happy City Initiative and CIC needs to gather and use certain information about individuals. These include employees, volunteers, partners, advisors, and other people via surveys that are conducted for research purposes.

This policy describes how this personal data must be collected, handled, stored and shared to meet the company's privacy data protection standards, and to comply with the law.

Why this policy exists

This data protection policy ensures Happy City Initiative and CIC:

- Complies with GDPR privacy and data protection law and follows good practice
- Protects the rights of employees, volunteers, partners, and any other people whose personal data we keep
- Is open about how it stores, shares and processes individuals' data
- Protects itself from the risks of a data breach

GDPR Law 2018

GDPR Law 2018 describes how organisations - including Happy City Initiative and CIC - must collect, store, handle and share personal information.
These rules apply regardless of whether data is stored electronically, on paper or on other materials.
To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.
GDPR 2018 is underpinned by **eight important principles**. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than the duration that we have set and shared
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways

8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Policy scope

This policy applies to all data that the company holds relating to identifiable individuals. This comprises:

- Name
- Postcode and address
- Email address
- Telephone number
- Photo
- Personal Identification Numbers
- Cultural identity
- Social identity
- Genetic identity
- Economic status
- IP address
- Mobile device identifier
- Geo-location
- Biometric data
- Psychological identity

Data protection risks

This policy helps to protect Happy City Initiative and CIC from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Happy City Initiative and CIC has some responsibility for ensuring data is collected, stored and handled appropriately.
Each team that handles personal data must ensure that it is handled and processed in line with this policy and the law.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that Happy City Initiative and CIC meets its legal obligations.

- The **data controller** is responsible for:

    - Keeping the board updated about GDPR privacy and data protection responsibilities, risks and issues.
    - Reviewing all GDPR procedures and related policies, in line with an agreed schedule.
    - Arranging GDPR training and advice for the people covered by this policy.
    - Handling GDPR questions from staff and anyone else covered by this policy
    - Dealing with requests from individuals to see the data Happy City Initiative and CIC holds about them (also called ‘subject access requests’).
    - Checking and approving any contracts or agreements with third parties that may handle the company’s sensitive data.
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.
    - Approving any data protection statements attached to communications such as emails and letters.
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

- The **data processors**, are responsible for:

    - Ensuring security processes are followed when equipment and computers are used to export and clean the data.
    - Adhering to Happy City Initiative and CIC GDPR privacy and data protection policy when dealing with partners and third-party services.

General staff guidelines

- The only people able to access personal or sensitive data 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 the data controller and the data processors.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below:
    - Install a firewall and virus-checking on your computers (this includes personal laptops and devices that employees, interns and volunteers bring and use in the office to do work for Happy City).
    - Make sure that your operating system is set up to receive automatic updates.
    - Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
    - Encrypt any personal information held electronically that would cause damage or distress, and constitute a break in the law if it were lost or stolen.
    - Do not keep copies of files with personal information on your computer's desktop. Always work in the G-Drive.This way, if you lose your computer, you don't lose the information.
    - Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
    - Consider installing an anti-spyware tool. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.
    - Strong passwords must be used and they should never be shared.
    - Personal data should not be disclosed to unauthorised people, either within the company or externally.
    - Data should be regularly reviewed and updated as per GDPR requirements. If subjects have requested that it be removed, or the data is no longer of use to us, it must be deleted and disposed of in a timely fashion.
    - Employees should request help from the data controller or the data processors if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be protected by strong passwords that are changed regularly and never shared between employees - with the exception of the Data Controller and data processors.
- If data is stored on removable media (like a USB stick), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services - GDrive is one of them.
- Servers containing personal data should be sited in a secure location - Happy City currently uses GDrive and AWS (Amazon Web Services).
- Data should never be saved directly to laptops or other mobile devices, except from the times when the data coordinators and / or other designated Happy City staff work with the data directly. When the work is done the files will be removed permanently from laptops or other mobile devices.
- All servers and computers containing data are protected by approved security software and a firewall.
- Happy City makes automatic updates to both our OS and CMS via Elastic Beanstalk. We are auto-notified of updates and a manual check is also made. Our Lavarel 3 platform is safe from common SQl injection and XSS attacks. We pen test every six months. We conduct a Nessus scan to check for vulnerabilities.

Data use

Personal data is of no value to Happy City Initiative and CIC unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. In particular, it should **never be sent by email**, as this form of communication is not secure.
- Personal data should never be transferred outside of the European Economic Area, unless we use organisations and systems that have already obtained approval from EU data protection authorities (for example we use AWS to store our Happiness Pulse data. For more information go here.)
- Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data, and if needs be make copies to work with on the Drive. There may be situations where making a copy of a file on a person's desktop is necessary. In these cases ensure that this copy is worked on as quickly as possible before you save a version of it on the Drive, then delete this forever from your desktop.

Data accuracy

The law requires Happy City Initiative and CIC to take reasonable steps to ensure data is kept accurate and up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a person's details when they call.
- Data should be updated as inaccuracies are discovered. For instance, if a person can no longer be reached on their stored telephone number / email address, it should be removed from the database.

NOTE: In the case of survey data, as we cannot contact people to ensure accuracy of data, we assume that what people fill in about themselves is correct.

Subject access requests

All individuals whose personal data is held by Happy City Initiative are entitled to:

- Ask what information the company holds about them and why
- Ask for their data to be deleted
- Be informed how to keep it up to date
- Be informed how the company is meeting its data protection obligations

If an individual contacts the company requesting this information, this is called a **subject access request**.
Subject access requests from individuals should be made by email, addressed to the data controller at info@happycity.org.uk.
Individuals will be charged £10 per subject access request. The data controller will aim to provide the relevant data within 14 days.
The data controller will always verify the identity of anyone making a subject access request before handing over any information.

NOTE: In the case of people taking part in a survey, we will try our best to identify them and remove their data from our database, if they request us to do so. This may not always be successful, as there may not be enough identifiers, such as an email address, to ensure we are removing data of a particular person.

Disclosing data for other reasons

In certain circumstances, GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.
Under these circumstances, Happy City will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Providing information

Happy City Initiative and CIC aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights
- What data we keep
- How long we undertake to keep it before seeking permission to continue to keep it

To these ends, Happy City has a privacy policy, setting out how data relating to individuals is used by the company.

NOTE: This is available on request. A version of this statement is also available on the company's website.

Sending data to authorised external contacts

When sending data to our clients and partners (for example the Happiness Pulse survey raw data and analyses) the following process must be followed:

1. Send our Policy to the client/partner(s) (ensure you export it in PDF format and send that)
2. Agree a Data Sharing agreement with the client/partners as appropriate
3. Ask the client/partner(s) to share their GDPR Policy via email, as we must ensure that they also adhere with GDPR
    a. If a client/partner doesn't have their own internal Data Protection Policy to send point them to this page on the government site, ask them to confirm in an email that they understand the legislation and will adhere to it.
4. Send the data by sharing an encrypted file via Google Drive. Once we get confirmation from our partner of a direct contact number we will then provide a unique password via telephone to access the encrypted file.

Data security breaches

All staff must report any data security breach to the data controller immediately they become aware of it, and without undue delay. The data controller must notify the supervisory authority of a personal data breach within 72 hours of learning about the breach. The notification should lay out the nature of the breach, the categories and approximate number of individuals impacted and the contact information of our data controller. Included should be the likely consequences of the breach, and what the controller has done to address and mitigate the breach.

The data controller must notify individuals ‘when the personal data breach is likely to result in a high risk to the rights and freedoms of individuals’ and they must do so without undue delay. This notification should include the contact information of Happy City’s data controller, the likely outcomes of the breach and how we plan on rectifying the situation.

Confirmation of reading

Please complete the details below and return to info@happycity.org.uk.

I confirm that I have been made fully aware of, understand, and have complied with the contents of the Data Protection Policy and Procedures for Happy City Initiative and CIC.

Name :

Signature:

Date:

Signed by Chief Executive

Date