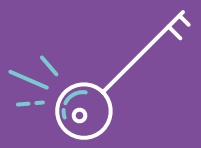
Social Change UK
Research and marketing that matters

How we protect data and privacy.

ICO REGISTRATION NUMBER: **Z3172576**
Updated **February 2020**

Key details.



Policy prepared by: Kelly Hunstone, Director

- Approved by board / management on: 01 May 2018 (updated)
- Policy became operational on: 01 May 2018
- Next review date: 01 April 2021

Data controller: Kelly Hunstone
Data processor: Eloise Pinchera

Introduction.

Social Change UK needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data is collected, handled and stored to meet the company's data protection standards — and to comply with the law (GDPR).

Why this policy exists.

01

This policy ensures Social Change UK:

- Complies with the **General Data Protection Regulations (GDPR)** and follows good practice;
- **Protects the rights** of staff, customers, stakeholders and partners;
- Is open about how it stores and processes **individuals' data;**
- **Protects itself** from the risks of a data breach.

The law (GDPR).

02

GDPR describes how organisations - including Social Change UK - must collect, handle and store 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.

The GDPR is underpinned by the following important principles. 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 necessary;
6. Be processed in accordance with the rights of data subjects;
7. Be protected in appropriate ways; and
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

The GDPR includes the following rights for individuals:

1. The right to be informed;
2. The right of access;
3. The right to rectification;
4. The right to erasure;
5. The right to restrict processing;
6. The right to data portability;
7. The right to object; and
8. The right not to be subject to automated decision-making including profiling.

GDPR and personal data.

03

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data.

04

The GDPR refers to sensitive personal data as "special categories of personal data".

The special categories specifically include genetic data and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

Lawful basis for processing data.

05

There are six available lawful bases for processing data. Most lawful bases require that processing is 'necessary'. If we can reasonably achieve the same purpose without the processing, we will not process data. We always determine the lawful basis before we begin processing, and we document it in a 'data processing' spreadsheet held and controlled by the data controller.
The lawful basis for processing data will fall under one or more of the following categories:

- Consent
- Contract
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Consent

Under GDPR, by consent, we mean that you provide agreement to give Social Change UK some of your personal information (i.e. address or phone number) or for Social Change UK to gather and use some of your personal information for specific purposes. **We make sure that consent is:**

1. Positively given (we only ask you to opt-in to provide information, not opt-out);
2. Reasonably specific and informed (we will let you know how we are planning to use your information); and
3. Given in line with your understanding that you have the right to withdraw consent and that this is easy to do.

Under this category, we obtain, record and manage consent through making consent requests prominent, concise and separate to other terms and conditions so that it is easy to understand when we are asking for this. **We will include:**

1. Our name (Social Change UK);
2. The name of any third-party controllers who will rely on the consent;
3. Why we want the personal data (the purpose);
4. What we will do with it (how we will use, and process it); and
5. How you can withdraw your consent at any time.

We keep consent requests under review and refresh them if anything changes by building regular consent reviews into our business processes.

Contract

Sometimes it is necessary, in order to perform our business functions, to process personal data to enter into and/or perform a contract with a data subject (the person who has given us their personal information). This contract may be for the provision or receipt of services (such as research or marketing services) or to allow us to obtain remuneration for these services.

Under this category, we would only process data when it is 'necessary' to perform a contract and is targeted and a proportionate step which is integral to deliver the contractual service or take the requested action. For example, the controller may process your address or email address to be able to deliver a particular good or service to you.

Legal obligation

Sometimes it may be necessary to process data in compliance with a legal obligation. This means that we may need to process personal data to comply with a common law or statutory obligation. We will identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out our obligations in this instance.

Sometimes it may be necessary to process data in compliance with a legal obligation. This means that we may need to process personal data to comply with a common law or statutory obligation. We will identify the specific legal provision or an appropriate source of advice or guidance that clearly sets out our obligations in this instance.

Under this category, we would only disclose the information you provide to comply with the law. This must be laid down either by UK or EU law, and can be either a statutory or a common law obligation.

For example, this could be to process data in order to submit a report to the National Crime Agency, Police or other law enforcement organisation in the UK or EU that there is knowledge or suspicion that a person is engaged in or attempting modern-day slavery, fraud, bribery or other criminal activity.

Vital interests

In rare instances, it may be necessary to process personal data to protect someone's life. In this case, the processing of personal data must be necessary and only used as a basis to process data in relation to interests that are essential for someone's life.

Under this category, as there is limited scope of applicability, we would only generally apply this to matters of life and death. For example, if someone is admitted to A&E with life-threatening injuries, the disclosure of any known allergies or long-term health conditions is necessary to protect their vital interests.

Public task

Sometimes, it may be necessary to process personal data where:
"processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."
(GDPR Article 6(1)(e).

This covers public functions and powers set out in law or to perform a specific task in the public interest that is set out in law. This basis is most relevant to public authorities, and any organisation including Social Change UK that carries out tasks in the public interest.

This category can be applied if we:

- Carry out a specific task in the public interest that is laid down by law; or
- Exercise official authority (for example, a public body's duties) which is laid down in law.

We would only process data under this category if the relevant task is laid down by UK or EU law and in exercising official authority or carrying out a specific task in the public interest. We may occasionally process data under this basis, for example, in the carrying out of functions of public administration, such as a resident survey for a local authority to be able to understand a public service or function to then act on recommendations for improvements.

Legitimate interests

This is likely to be the most appropriate basis for processing personal data. In using this basis, we take on extra responsibility to consider and protect people's rights and interests.

There are three elements to the legitimate interests' basis. These are:

- Identifying a legitimate interest;
- Showing that the processing is necessary to achieve this; and
- Balancing it against the individual's interests, rights and freedoms.

These legitimate can include interests of Social Change UK and can include commercial interests, individual interests or wider societal benefits.

As with all bases for processing, the processing must be necessary, and we will balance our interests against the individual's interests. If they would not reasonably expect the processing or it would cause unjustified harm, we will not proceed.

Cases where we may process personal data under this basis include, for example, if you have signed up to stay up to date about our research work, we may send you a copy of an online report or white paper relevant to our research expertise. This would be a legitimate basis linked to your interest in our work and could support our future business in forming a working relationship with yourself.

Privacy.

06

Social Change LTD may use and share the information you provide and other information held about you for the purposes set out below.

Websites and online tools owned and managed by Social Change UK:

When you create or log in to an online account you agree to our privacy policy (this document) and cookie notice (pages 10-12). Information collected from your use of our websites or our mobile applications will be processed in accordance with this document.

Privacy Notice

Information we may hold about you

- Information you've provided to us willingly;
- Information about products and services you've ordered or enquired about;
- Information provided by other companies who have obtained your permission to share information about you;
- Information about your interaction with adverts and services such as registration, comments on social media etc;
- Information we collect using cookies stored on your device (for example, this may be a PC, phone or tablet) about your use of the Social Change UK and/or selected third party websites we own and manage. (For more information on cookies and how to manage them, please see our cookies notice on pages 10-12);
- Your IP address, this is a number that identifies a specific network device on the internet and is required for your device to communicate with websites;
- Technical information from your device relating to the service you receive.

Please do not submit your personal information to us if you do not wish us to collect it.

Message boards, blogs and other public forums

The websites we own and manage make message boards, blogs and other such user generated content facilities available to users of the Site(s) and registered users can provide content for, and participate in these facilities. Any information that is disclosed in these areas of our Site becomes public information and you should always be careful when deciding to disclose your personal information.

Email a friend and share this article facilities

When an individual uses these facilities and provide us with personal data (e.g. the name and email address) of a third party, please ensure that you have their consent before giving us their details.

How we may use your information

By using our website(s), you agree that we may collect, hold, process and use your information (including personal information) for the purpose of providing you with the Site services and developing our business which shall include (without limitation):

- Verifying your identity (for example when you return to the Site);
- Personalising your visits to the Site and developing the design and style of the Site to improve the services provided to you Informing you about the latest changes to the Site, or products, services or promotional offers that you might find interesting;
- Dealing with, and responding to you about, a comment you have submitted for or on our message boards, blogs and other such user generated content facilities;
- Enabling you to share our content with others e.g. using our 'Email a friend' and 'Share this article' facilities;
- Informing you if you have been successful in any Site competitions or promotions;
- Compiling customer reviews;
- Conducting market research; and
- Carrying out statistical, technical and logistical analysis.

According to your preferences, communicating (and personalising such communication) with you:

- To send you periodic newsletters about your chosen services;
- To send you direct marketing. This may include communications by post, telephone or email or SMS about us and our business partners' products and services, events and special offers, including where applicable, for a reasonable time;
- To provide you with personalised services, such as providing with you with viewing recommendations and tailored advertising. This includes where we have agreement to store information about you on the devices you use, for example to make some of the adverts you see more relevant to you (if applicable); and
- To provide you with advertising more relevant to your interests and your online behaviour through the use of cookies when you visit our website(s).

Subject to obtaining your consent, we may also supply personal information about you to third parties. We may transfer, sell or assign any of the information described in this policy to third parties as a result of a sale, merger, consolidation, change of control, transfer of assets or reorganisation of our business.

Marketing.

07

Online Behavioural Advertising (OBA)

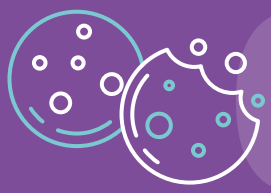
If you do not want to receive online advertising where this advertising is relevant to your interests, or don't want information processed through the use of cookies, please see the section below on cookies.

Advertising Services

We gather anonymous information such as on the types of pages visited, and keywords searched on in order to build an overall, but anonymous, picture of interests or preferences based on individual users browsing habits so that we can offer a more personal experience. To this information, we include information relating to a user's country, region and connection type gathered from elements of the IP of the browsing device. This practice is a core method used by Social Change UK to make our content more relevant to viewers.

For more information about interest based advertising and how to turn this feature off, please see our cookies notice below.

Cookies.



08

You should be aware that when you use our website, mobile sites or mobile apps, our website uses 'cookies' to collect key information which will help to provide you with a good user experience.

What are cookies and how do they work?

Cookies are small bits of text that are downloaded to your computer or mobile device when you visit a website. Your browser sends these cookies back to the website every time you visit the site again, so it can recognise you and can then tailor what you see on the screen.

What do you use cookies for?

Cookies are an important part of the internet. They make using websites much smoother and affect lots of the useful features of websites. There are many different uses for cookies, but the ones our sites use fall into the following groups:

- Strictly necessary cookies
- Analytical/performance cookies
- User experience cookies
- Session cookies
- Third party cookies

Here are some examples of essential cookies:

- Cookies that allow the website to remember choices you make, such as your language or region and to provide improved features;
- When you add something to the online shopping basket, cookies make sure it's still there when you get to the checkout; and
- Improving your browsing experience.

Here are some ways in which cookies improve your browsing experience:

- Remembering your preferences and settings, including marketing preferences;
- Remembering if you've filled in a survey, so you're not asked to do it again;
- Remembering if you've been to the site before. If you are a first-time user, you might see different content to a regular user;
- Restricting the number of times you're shown a particular advertisement. This is sometimes called 'frequency capping';
- Showing you information that's relevant to products of ours that you have;
- Enabling social media components, like Facebook or Twitter;
- Showing 'related article' links that are relevant to the page you're looking at;
- Remembering a location you've entered such as weather forecasts; and
- Analytics (see more under 'analytics cookies').

Strictly necessary cookies

These are cookies that are required for the operation of our site and allow you to use all of the different sections and functions of it. Examples include cookies that enable you to log into secure areas of our site and keep you logged in during your visit. Without these cookies, services and functions you've asked for cannot be provided.

First-party cookies

These are cookies that are needed to provide the service you have asked for. Some cookies are essential, so you can move around the website and use its features. Without these cookies, services you've asked for can't be provided. These cookies don't gather information about you that could be used for marketing or remembering where you've been on the internet.

Analytical/performance cookies

We like to keep track of what pages and links are popular and which ones don't get used so much to help us keep our sites relevant and up to date. It's also very useful to be able to identify trends of how people navigate (find their way through) our sites and if they get 'error messages' from web pages. This group of cookies are used to gather this information. These cookies don't collect information that identifies you. The information collected is anonymous and is grouped with the information from everyone else's cookies. We can then see the overall patterns of usage rather than any one person's activity. Analytics cookies only record activity on the site you are on and they are only used to improve how a website works.

User experience cookies

These cookies are used to improve your user experience by enabling the site to 'remember' you and distinguish you from other users, either for the duration of your visit (using a 'session cookie') or for repeat visits (using a 'persistent cookie'). They enable you to navigate between pages efficiently, storing your preferences and generally improve your experience of the site.

Session cookies

These are also known as 'temporary cookies' and help the site to recognise users and the information provided when they navigate through a website. These cookies only retain information about a user's activities for as long as they are on the site. Once the web browser is closed, the cookies are deleted.

Third-party cookies

These cookies are set by someone other than the owner of our website, for example, webpages that contain content from other websites such as YouTube or Twitter which may set their own cookies. If you share a link to a page from our website, the service you share it on may set a cookie to your browser. Within third-party cookies, we also use 'affiliate' cookies. Some of our web pages will contain promotional links to other companies' sites. If you follow one of these links and then register with or buy something from that other site, a cookie is sometimes used to tell that other site that you came from one of our sites.

support.google.com/analyticsanswer/7667196

Research services.

08

Why we hold personal data for research

We need to know and use certain personal data for a number of reasons within our research services:

- to be able to understand how your views and experiences link into the topic being researched, so we can analyse the findings and generate more accurate insights;
- to be able to contact you at a later stage of the research for any additional input on the topic;
- to be able to clarify anything you have told us to in relation to the research topic to ensure we have fully understood your views;
- to be able to clarify anything you have told us in relation to yourself and to ensure that our records are accurate and up to date;
- to be able to process and send you an incentive for participating (as appropriate), and
- to be able to contact you about any future research that may be of interest or of relevance to you (if you choose to be contacted).

How we use and process personal data within research

We anonymise all information by removing names and other personal data that could identify you from all of our research outputs, including reports and other communications.

Some characteristics that cannot explicitly identify you as an individual, such as age range, location, gender or occupation, may be included to support the research findings. We will always first ensure that any characteristics included cannot be used to identify you as an individual.

The only people who will have access to your personal data are those who need it for their work, and we do not share it informally within Social Change UK or outside of the company.

The only exception to this is where we are contractually required or required by law to inform any relevant organisations (page 20) – this may be in the form of liaising with the authorities or as part of a Data Sharing Agreement (DSA). Relevant information regarding any data sharing will be shared with participants ahead of conducting the research. We ask everyone to complete a consent form before taking part in our research, and we only use your personal data for the explicit purpose(s) outlined in the consent form. In order to claim a research incentive, we ask that participants sign a form as receipt of the incentive. This form will capture personal information including, but not limited to:

- Full name
- Postal address
- E-mail address
- Telephone / mobile number
- Signature

Participants taking part in research are also given the option of joining our research panel, which can be achieved by completing a participant form. This is optional and is not essential to be able to participate in research projects with Social Change UK.

Our research team follow Social Change UK's overall guidelines and policies for secure data storage, data protection and data accuracy (page 14 onwards).

People, risks and responsibilities.

09

Policy scope

This policy applies to:

- The head office of Social Change UK (29-31 Mint St, Lincoln, LN1 1UB);
- All branches of Social Change UK (Gridiron Building, 1 Pancras Square, London, N1C 4AG;
- All staff and volunteers of Social Change UK; and
- All contractors, suppliers and other people working on behalf of Social Change UK.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR.

This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- ...plus any other information relating to individuals.

Data protection risks

This policy helps to protect Social Change UK 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; and
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities.

10

Everyone who works for, or with Social Change UK 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 data protection principles.

However, these people have key areas of responsibility:

The board of directors is ultimately responsible for ensuring that Social Change UK meets its legal obligations.

The data protection officer, Kelly Hunstone, is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and related policies, in line with an agreed schedule;
- Arranging data protection training and advice for the people covered by this policy;
- Handling data protection questions from staff and anyone else covered by this policy;
- Dealing with requests from individuals to see the data Social Change UK 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.

The IT manager, David Stanton, is responsible for:

1. Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
2. Performing regular checks and scans to ensure security hardware and software is functioning properly; and
3. Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

The marketing team, led by Kelly Hunstone is responsible for:

1. Approving any data protection statements attached to communications such as emails and letters;
2. Addressing any data protection queries from journalists or media outlets like newspapers; and
3. Where necessary, working with other staff to ensure marketing initiatives abide by the GDPR.

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 managers;
- **Social Change UK 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 below;
- 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 company 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; and
- **Employees should request help from their line manager or the data protection officer** if they are unsure about any aspect of data protection.

Data storage.

12

These rules describe how and where data is safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper,** it is kept in a secure place where unauthorised people cannot see it.

The following apply to data that is usually stored electronically but has, or could be printed out for some reason:

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

When **data is stored electronically,** it is protected from unauthorised access, accidental deletion and malicious hacking attempts. **We ensure the following:**

- Data is **protected by strong passwords** that are changed regularly and never shared between employees;
- If data is **stored on removable media** (like a CD or DVD), these are kept locked away securely when not being used;
- Data is only stored on **designated drives and servers,** and only uploaded to an **approved cloud computing service(s)**;
- Servers containing personal data are **sited in a secure location**, away from general office space;
- Data is **backed up frequently**. Backups are tested regularly, in line with the company's standard backup procedures;
- Data is **never saved directly** to laptops or other mobile devices like tablets or smart phones; and
- All servers and computers containing data are protected by **approved security software and a firewall.**

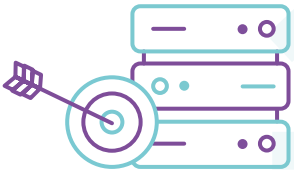
Protecting data.

13

We ensure the following:

- When working with personal data, employees ensure **the screens of their computers are always locked** when left unattended;
- Personal data **is not shared informally**. In particular, it should never be sent by email, as this form of communication is not secure;
- Data considered personal or identifiable is **encrypted before being transferred electronically**;
- Personal data is **never be transferred outside of the European Economic Area**; and
- Employees **do not save copies of personal data to their own computers.**

Data accuracy.



14

The law requires Social Change UK 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.

Our commitment:

- 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 customer's details when they call; and
- Social Change UK will make it **easy for data subjects to update the information** Social Change UK holds about them. For instance, via the company website or email campaign.

Data breach.

15

The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. We only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Subject access requests.

All individuals who are the subject of personal data held by Social Change UK are entitled to:

- Ask **what information** the company holds about them and why;
- Ask **how to gain access** to it;
- Be informed how to **keep it up** to date; and
- 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:

hello@social-change.co.uk

The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will not be charged if they make a subject access request. However we can refuse or charge for requests that are manifestly unfounded or excessive. The data controller will aim to provide the relevant data within 21 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information such as a request to see a passport or driving licence to verify they are who they say they are.

Individuals have a right to complain to the Information Commissioners Office (ICO) if they think there is a problem with the way we are handling their data.

Please visit www.ico.org.uk for more information.

Disclosing data for other reasons.

17

In certain circumstances, the GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Social Change UK 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.

18

Social Change UK 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

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

This is available here:

www.social-change.co.uk/privacy

We only work with organisations that want to bring about positive social change, and people who want to do good. We think this is you... let's talk.

Social Change UK
Research and marketing that matters

FOLLOW US

London.

The Gridiron Building,
1 Pancras Square,
London,
N1C 4AG

Phone: 020 7186 1980

Lincoln.

First floor,
29-31 Mint Street,
Lincoln,
LN1 1UB

Phone: 01522 77 50 60

www.social-change.co.uk