Data protection & IT policy

Last updated January 2020

Contents

1/ Scope

This policy applies to all personal data processed by the Company and applies to employees, interns and freelancers undertaking work for Citizens 4 Change. Violations of this policy will be documented and can lead to disciplinary action.

The organisation may seek legal remedies for damages incurred as a result of any violation and may be required by law to report certain illegal activities to the proper enforcement agencies.

The Chief Executive Officer shall take responsibility for Company compliance with this policy.

2/ Legislation

All users shall comply with the relevant legislation. This includes the following:

Data Protection Act 1998 / the General Data Protection Regulations (GDPR).

The Company processes data in accordance with its responsibilities under the General Data Protection Regulation (EU) 2016/679 (GDPR). Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Computer Misuse Act 1990. This Act makes it an offence to try and access any computer system for which authorisation has not been given.

Copyright Design and Patents Act 1988. Under this Act it is an offence to copy software without the permission of the owner of the copyright.

Defamation Act 1996. Under this Act it is an offence to publish untrue statements which adversely affect the reputation of a person or group of persons.

Terrorism Act 2006. This Act has makes it a criminal offence to encourage terrorism and/or disseminate terrorist publications.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. This allows for any organisation to monitor or record communications (telephone, internet, email, and fax) for defined business related purposes.

Types of information

We distinguish between the different types of information that we gather.

Personally Identifiable Information (PII) describes any information that could be used to identify a person either directly or indirectly. It includes names and contact details, and case studies or interviews which include the individual's full name or sufficient detail about an individual's life that someone might reasonably identify them even if the name is omitted.

PII: Sensitive Information. There are special categories of PII in the GDPR regulations that are considered sensitive. This includes data about health, race or ethnicity, political opinions, Religion or philosophical beliefs or sexual behaviour or sexual orientation.

Non-Personally Identifiable Information includes short quotes or extracts from interviews with no names or identifying characteristics, statistics or general research findings and insights, and backend data generated by our online platforms such as number of users accessing a particular story.

3/ Seeking informed consent

We seek consent when we collect any of these three types of information. To ensure that consent is valid and enforceable we explain:

- Why are we collecting the information – we explain clearly our reasons for requesting information so that we can achieve our objectives. We avoid collecting information we don't need.
- What we will do with the information,
- How we will store the information,
- When we will we stop using the information,
- Where proof of consent is stored and how can we access it.

To satisfy the requirement for informed consent we explain:

- Who we are and how we can be contacted if a person has questions. Every consent form contains a telephone number and/or e-mail for people to contact if they have any questions or wish to withdraw consent.
- What information we are going to collect and why, explicitly flagging any sensitive information that may be requested.
- We always make clear that if a report of harm towards a child is made we will escalate this report to the authorities.
- What we plan to do with the information.
- Who we will share the information with and how.
- How long we plan to keep any PII and how we will keep it secure.

The above information must be presented in a way that is clear, intelligible and adapted for the intended audience - if we do not meet this requirement, the consent is not valid. Therefore, we take all reasonable steps to ensure the person understands what they are signing by

- Using the local language.
- Avoiding technical language.
- Presenting information in a user-friendly format.
- Providing a copy of the consent form or the option to download online consent information so the person can refer back to the terms of consent and contact us if they are unhappy or wish to withdraw consent.

Storage of proof of consent

If requested, we must be able to provide evidence that adequate information was shared by us and informed consent provided. If we have obtained consent but can't link it to the PII that we have collected, it means that we do not have consent.

To satisfy this requirement, we retain copies of (offline) consent forms for any PII we are collecting, storing or using; and ensure that these are linked to the individuals' records in our database. We only keep records of individuals in the database who have explicitly given consent [recorded in their survey response] to us retaining their data.

Use of information

We will only share Non-Personally Identifiable Information. Under no circumstances will we share Personally Identifiable Information, or Sensitive Personally Identifiable Information.

The only situation when we will share Sensitive Personally Identifiable Information is when there is a suspicion that a child is being harmed. In that situation a formal report will be made to the Authorities.

Individuals whose images are used on our websites or publicity materials are contacted annually to consent for their images to still be used.

Access to people's PII will be restricted to staff who have signed a commitment to securing our data.

Retention of data

We will keep data for the shortest possible use of time. This requires us to

- Send out an annual request to individuals to update their PII and / or withdraw their consent to sharing their data with us.
- There is an accessible unsubscribe button on our website. When someone unsubscribes all of their data is deleted.
- Archiving the data of individuals who have not engaged with us during the previous year.
- Non-PII data that informs research publications is retained but archived as soon as the research assignment is completed.

Adhering to standards

Every year we assess our adherence to data protection standards using the ICO's Data protection self-assessment
https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

4/ Informed consent to the collection of children's data.

We may collect Personally Identifiable Information, Sensitive Information or Non-Personally Identifiable Information about children from adults in their lives, or directly from children.

When collecting information about children from adults we make it clear as part of the informed consent process that if a report of harm towards a child is made we will escalate this report to the authorities.

GDPR regulations require proof of parental consent for personal information collected from children under the age of 13. The requirement for parental consent may, however, vary under specific circumstances

- If we are collecting Non-Personally Identifiable Information (e.g. general insights from children and young people without recording names or identifying details) we may collect consent from a "responsible adult" such as a teacher or youth leader. This does not apply for Personally Identifiable Information or the collection of sensitive information.
- Where we are collecting Personally Identifiable Information but the parent is unavailable, we must be able to show that we have taken all reasonable steps to

obtain their consent. If this proves impossible, consent may be provided by a responsible adult who has an ongoing relationship with the child.
- If we are collecting sensitive information and the parent is unavailable, we should not include that child/young person in the data collection sample.
- When planning digital channels, we need to limit the information gathered about children to Non-Personally Identifiable Information so that we do not need to meet the requirement for parental authorisation.

5/ Children as Citizens 4 Change

GDPR Regulations enable us to identify and communicate with children from 13 years who are Citizens 4 Change without requiring parental consent. We target secondary-school age children, who have a degree of digital literacy and access to phones.

Childrens' rights to online privacy and freedom of expression

As an organization guided by the best interests of the child[1] we are governed by a set of general principles that advance children's rights to online privacy and freedom of expression[2]

- Children have the right to privacy and the protection of their personal data.
- Children have the right to freedom of expression and access to information from a diversity of sources.
- Children have the right not to be subjected to attacks on their reputation.
- Children's privacy and freedom of expression should be protected and respected in accordance with their evolving capacities.
- Children have the right to access remedies for violations and abuses of their rights to privacy and free expression, and attacks on their reputation.

To protect children's online rights and to comply with GDPR when processing children's personal data, the Company is required to adopt the following measures.

Data protection by design and default

From the outset the Company designs data protection measures, messaging & communications with children in mind. We put in place appropriate technical and organizational measures to implement the data protection principles and safeguard individual rights. We integrate data protection into our processing activities and business practices, from the design stage right through the lifecycle.

We invite the views of children to feedback on our processes, communications & services; so that they help us to identify the risks and design safeguards. This is consistent with the

[1] CRC, Article 3.
[2] UNICEF Industry toolkit 2018: Children's online privacy and freedom of expression

UN Convention on the Rights of the child which provides at Article 12 that every child has the right to express their views, feelings and wishes in all matters affecting them, and to have their views considered and taken seriously.

Children have rights over their data.

- Children have the same rights as adults under our Privacy Statement.
- Children's personal data is maintained so that it is accurate and up-to-date.
- Children have the right to access their personal data, to correct it or to request its erasure.
- Children have the right to object to the collection and processing of their data and have the right to opt out from receiving surveys and other communications.

Providing clear privacy notices for children.

So that they are able to understand what will happen to their personal data and what rights they have. These are written in a child friendly language, and make them aware of data protection, risks, consequences, safeguards and rights by:

- Telling them what we are doing with their personal data;
- Being open about the risks and safeguards involved; and
- Letting them know what to do if they are unhappy

This will also help them to make informed decisions about what personal data they wish to share.

Obtaining Informed consent from children.

Children have the same rights to data privacy as adults and the same principles of obtaining informed consent apply to them.

Keeping children's personal data to what is minimally necessary

Under the principle of data minimization, data collection on children should be limited to what is necessary for a specific purpose.

Verification of the child's age

We are required to make reasonable efforts to ensure that everyone providing their own consent is at least 13 years old. We will explore the viability of using the services of a third-party identity authentication providers to minimize the risks attendant to data collection; such as https://www.agechecked.com/charity/

Obtaining verifiable parental consent

Where necessary to engage with children under the age of 13, we will obtain consent from whoever holds parental responsibility for the child[3].

If it is necessary to engage with children under this age we will only do so in ways that collect non-personally identifiable information; and to do so via face to face interactions.

Where there are no systems in place to obtain parental consent, children under the age of 13 will be excluded from using the Company's online and SMS services.

Whilst, seeking out consent from a holder of parental responsibility over a child we will also let the child know that s/he has a right to withdraw that consent once they are competent to make such a decision.

We will obtain verifiable parental consent by:

- Providing a child with a consent form to be signed by the parent and returned to us as hard copies or electronically scanned versions of signed parental consent forms.
- Obtaining a parent's mobile phone number from a child, and sending a SMS message requesting their consent.
- Verifying a parent's identity by double checking with a form of government-issued identification.

6/ Internet and Email Usage Policy and Guidelines for Staff.

This policy sets out the obligations and expectations on employees of the Company including contractors and temporary staff, who use the Company's IT facilities. IT facilities are provided to assist with day to day work. It is important that they are used responsibly, are not abused, and that individuals understand the legal professional and ethical obligations that apply to them.

Authorisation

No person is allowed to use Company IT facilities who has not previously been authorised to do so by their supervisor. Unauthorised access to IT facilities is prohibited and may result in either disciplinary action or criminal prosecution.

[3] Someone who, according to the law in the child's country of residence, has the legal rights and responsibilities for a child that are normally afforded to parents. This will not always be a child's "natural parents "and parental responsibility can be held by more than one natural or legal person.

Responsibilities

All Users are expected to act in a manner that will not cause damage to IT facilities or disrupt IT services. Any accidental damage or disruption must be reported to their Supervisor as soon as possible after the incident has occurred. Users are responsible for any IT activity which is initiated under their username.

Use of the Internet by employees is encouraged where such use is consistent with their work and with the goals and objectives of the Company in mind. Reasonable personal use is permissible subject to the following:

- Users must not participate in any online activities that are likely to bring the Company into disrepute, create or transmit material that might be defamatory or incur liability on the part of the Company, or adversely impact on the image of the Company.
- Users must not visit, view or download any material from an internet site which contains illegal or inappropriate material. This includes, but is not limited to, pornography (including child pornography), obscene matter, race hate material, violence condoning messages, criminal skills, terrorism, cults, gambling and illegal drugs.
- Users must not knowingly introduce any form of computer virus into the Company's computer network.
- Personal use of the internet must not cause an increase for significant resource demand, e.g. storage, capacity, speed or degrade system performance.
- Users must not "hack into" unauthorised areas.
- Users must not download commercial software or any copyrighted materials belonging to third parties, unless such downloads are covered or permitted under a commercial agreement or other such licence.
- Users must not use the Internet for personal financial gain.
- Users must not use the Internet for illegal or criminal activities, such as, but not limited to, software and music piracy, terrorism, fraud, or the sale of illegal drugs.
- Users must not use the Internet to send offensive or harassing material to other users.
- Use of gambling sites, online auction sites and other such inappropriate websites is not permissible. If you are in any doubt, you should confirm with your supervisor whether a site is permissible or not before accessing the site.

- Staff may face disciplinary action or other sanctions (see below) if they breach this policy.

Use of Email / Instant Messaging

Messages sent or received on the Company email / IM system form part of the official records of the Company; they are not private property. The Company does not recognise any right of employees to impose restrictions on disclosure of such messages within the Company. These may be disclosed through legal obligations, as part of legal proceedings (e.g. tribunals), and as part of disciplinary proceedings. Users are responsible for all actions relating to their IT account including username and password, and should therefore make every effort to ensure no other person has access to their account.

When using Company email, users must:

- Ensure they do not disrupt the Company's wider IT systems or cause an increase for significant resource demand in storage, capacity, speed or system performance e.g. by sending large attachments to a large number of internal recipients.
- Ensure they do not harm the Company's reputation, bring it into disrepute, incur liability on the part of the Company, or adversely impact on its image.
- Do not seek to gain access to restricted areas of the network or other "hacking activities" is strictly forbidden.
- Must not use email for the creation, retention or distribution of disruptive or offensive messages, images, materials or software that include offensive or abusive comments about ethnicity or nationality, gender, disabilities, age, sexual orientation, appearance, religious beliefs and practices, political beliefs or social background. Employees who receive emails with this content from other employees of the Company should report the matter to their supervisor.
- Do not send email messages that might reasonably be considered by recipients to be bullying, harassing, abusive, malicious, discriminatory, defamatory, and libellous or contain illegal or offensive material, or foul language.
- Do not upload, download, use, retain, distribute, or disseminate any images, text, materials, or software which might reasonably be considered indecent, obscene, pornographic, or illegal.
- Do not engage in any activity that is likely to
    - Corrupt or destroy other users' data or disrupt the work of other users.

    - Waste staff effort or Company resources, or engage in activities that serve to deny service to other users.
    - Be outside of the scope of normal work-related duties – for example, unauthorised selling/advertising of goods and services.
    - Be a breach of copyright or license provision with respect to both programs and data, including intellectual property rights.
- Do not send chain letters or joke emails from a Company account.

Staff who receive improper email from individuals inside or outside the Company, should discuss the matter in the first instance with their supervisor.

Personal use of a Company email / message account is not permitted.

Email Good Practice

The Company has good practice guidelines for dealing with email when staff are out of the office for longer than three days. When activating the "out of office" facility messages should name an alternative member of staff for correspondents to contact if necessary. This will ensure that any important messages are picked up and dealt with within required timescales.

During periods of absence when highly important emails are anticipated, the employee (or manager) should make arrangements for notification and access by another appropriate member of staff.

Where sensitive and confidential information needs to be sent via email for practical reasons, please be aware that email is essentially a non-confidential means of communication. Emails can easily be forwarded or archived without the original sender's knowledge. They may be read by persons other than those they are intended for.

Users must exercise due care when writing emails to avoid being rude or unnecessarily terse. Emails sent from the Company may be interpreted by others as Company statements. Users are responsible for ensuring that their content and tone is appropriate. Emails often need to be as formal and business-like as other forms of written correspondence.

Users should delete all personal emails and attachments when they have been read and should also delete all unsolicited junk mail. In the process of archiving emails, users should ensure inappropriate material is not archived

Caution should be used when opening any attachments or emails from unknown senders. Users must best endeavour to ensure that any file downloaded from the internet is done so from a reliable source.

Use of Social Media

Many Company employees will already be using social media in their personal lives. When you are not at work, it is, of course, entirely up to you to decide whether and how you choose to create or participate in a social media space or any other form of online publishing or discussion. This is your own business. The views and opinions you express are your own.

However, if you identify yourself as an employee of the Company or as being associated with it in any way, you must be mindful of this when participating in social media. We have a responsibility to make you aware that, even where you don't intend it, you can harm the company's business and reputation when using social media in a personal capacity, and that breaching this policy outside of work can still result in disciplinary action.

Legitimate Access to Prohibited Material

There may be circumstances where users feel that the nature of their work means that they are required to access or use material prohibited under this policy. If so, this should be discussed with their Supervisor. The Company is legally responsible for the content and nature of all materials stored on/accessed from its network.

Remote Users

Users may sometimes need to use Company equipment and access the Company network while working remotely. The standards set out in this document apply whether or not Company equipment and resources are being used.

Monitoring

All resources of the Company, including computers, email, and voicemail are provided for legitimate use. If there are occasions where it is deemed necessary to examine data beyond that of the normal business activity of the Company then, at any time and without prior notice, the Company maintains the right to examine any systems and inspect and review all data recorded in those systems. This will be undertaken by authorised staff only. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists in the management of information systems.

Penalties for Improper Use

Withdrawal of facilities. Users in breach of these regulations may have access to Company IT facilities restricted or withdrawn.

Disciplinary Action. Breaches of these regulations may be dealt with under the Company's disciplinary procedures. It may lead to termination of employment from the Company.

Breaches of the law. Where appropriate, breaches of the law will be reported to the police.

7/ Managing risk

Risk is intentionally and systematically managed on an ongoing basis. Data protection risks are a key concern. A quarterly survey is sent to all C4C team members asking them to identify the top three risks they envisage the Company facing; the risk category; likelihood and impact. These are then collated in a quarterly team meeting where we collectively reflect on the risk survey results and agree mitigation measures. The results are recorded in a risk register and dashboard.

8/ Policy Review

The effectiveness of this policy and associated arrangements will be reviewed annually under the direct supervision of the Company Chief Executive.

Appendix 1: Guidelines; What does GDPR require of us?

What information requires consent?

The General Data Protection Regulations (GDPR) came into force in May 2018. They place additional requirements on organisations and demand greater clarity about the type of information they gather and the consent that should be attached to it.

In planning what consent is needed, companies need to make a distinction about the different types of information that we gather:

Personally Identifiable Information (PII) describes any information that could be used to identify a person either directly or indirectly. Examples of PII include:

- Names and contact details (address, telephone numbers, e-mail addresses)
- Photos and video

- Case studies or interviews which include the individual's full name or sufficient detail about an individual's life that someone might reasonably identify them even if the name is omitted

In general, where PII is collected, evidence is needed of the individual's informed consent to collect, use and share this information.

PII: Sensitive Information. There are special categories of PII that are considered sensitive and particular care must be taken when collecting or using this type of information. Sensitive information is defined in the GDPR regulations as:

- Health
- Race or ethnicity
- Political opinions
- Religion or philosophical beliefs
- Sexual behaviour or sexual orientation
- Genetic or biometric data

Whenever there is an intention to gather sensitive information, it must be explained what is being collected and how it will be used, so that people can make an informed decision about whether they want to share this information or not.

Non-Personally Identifiable Information includes:

- Short quotes or extracts from interviews with no names or identifying characteristics
- Statistics or general research findings and insights
- Backend data generated by our online platforms such as number of users accessing a particular story

This information can be legally collected without consent.

Ensuring consent is valid and enforceable: The 'W' Questions

In order for consent to be valid and enforceable, we need to satisfy the five W' questions:
Why are we collecting the information?
What information did we provide when obtaining consent?
Who did we collect consent from?
When will we stop using the information?
Where proof of consent is stored and how can we access it?

Why are we collecting the information?

If we are collecting personal information we must have *explicit and legitimate* reasons for requesting it. To satisfy this requirement, we must:.

- Be able to justify why the information is important and how it will help us achieve our organisational objectives.
- Avoid collecting information we don't need - if we don't know how we are going to use it, we shouldn't be collecting it.

What information did we provide when obtaining consent?

In order to be binding, we must obtain *informed consent.* To satisfy this requirement, we must explain:

1. Who we are and how we can be contacted if a person has questions.
2. What information we are going to collect and why, explicitly flagging any sensitive information that may be requested.
3. What we plan to do with the information.
4. Who we will share it with and why.
5. How long we plan to keep any PII and how we will keep it secure.

The above information must be presented in a way that is *clear, intelligible* and *adapted for the intended audience*. If we do not meet this requirement, the consent is not valid. To satisfy this requirement, we must:

- Obtain consent in the local language.
- Avoid technical or legalistic language, especially when collecting consent from children, young people or individuals with low literacy levels.
- Set out the information in a user-friendly format, avoiding long and complex text.
- Take all reasonable steps to ensure the person understands what they are signing.
- Provide a copy of the consent form or the option to download online consent information so the person can refer back to the terms of consent and contact us if they are unhappy or wish to withdraw consent.

Who did we collect consent from?

The new data protection regulations require proof of *parental consent* for personal information collected from children under the age of 16.

The requirement for parental consent may, however, vary under specific circumstances:

- If we are collecting Non-PII we may collect consent from a “responsible adult” such as a teacher or youth leader.
- Where we are collecting PII but the parent is unavailable, we must be able to show that we have taken all reasonable steps to obtain their consent. If this proves impossible, consent may be provided by a responsible adult who has an ongoing relationship with the child.
- If we are collecting sensitive information and the parent is unavailable, we should not include that child/young person in the data collection sample.

Online Consent. Gaining parental consent is more complicated for online platforms. Asking girls to obtain parental consent may act as a barrier to them accessing the site or content and even if gained, parental consent is very difficult to verify. For this reason, when planning digital channels we need to limit the information gathered to non-PII so that we do not need to meet the requirement for parental authorisation.

When will we stop using the information?

We must state how long it is going to use PII on the consent form and this must be strictly adhered to unless an extension to the original consent is obtained. Once the agreed time period has been reached, we must:

- Delete/Destroy or archive and limit access.
- Take all reasonable steps to remove the images or information from our websites and social media platforms.

Even where consent has been given, the individual has the right to withdraw consent and ask for their PII to be removed. GDPR requires that withdrawing consent is as easy as giving it. This means that:

- Offline consent forms must include a phone number and/or e-mail that people can contact to remove their consent.
- If we are collecting PII online, there must be a clear and simple way to request for personal data to be removed
- We must have a way of tracking all personal information so that it can be removed if a request is received.

There is no restriction on the amount of time we can store and use Non-PII.

Where proof of consent is stored and how can we access it?

In order to be valid, consent must be *demonstrable* - that is, if requested we can provide evidence that adequate information was shared by us and informed consent provided. If we have obtained consent but can't link it to the PII that we have collected, it means that we do not have consent.

To satisfy this requirement, we must:

- Retain copies of (offline) consent forms for any PII we are collecting, storing or using. If consent has been obtained by a local partner we must ask them to provide scanned copies of all consent forms
- If PII is collected by a local partner or consultant who anonymises or aggregates the information before sharing it with us, we do not need to hold copies of consent but our contract explicitly state our expectation in terms of gathering consent
- In cases where we won't gather documented consent from individuals (e.g. roadshows, events) evidence of posters, signage and other information explaining that videos and photographs are to be taken must be stored as evidence of (implicit) consent.