Tell Us North CIC

Data Protection Policy

(Incorporating 2018 General Data Protection Regulation)

Contents

Document details and review

Organisation	Tell Us North CIC
Responsible person	Chief Executive
Date approved	January 2022
Reviewed	October 2021
Next review	October 2023

This policy will be reviewed every two years

1. Scope of the policy

1.1. This policy applies to all staff, associates, volunteers, and directors of Tell Us North.

2. Introduction

2.1. The purpose of this policy is to enable Tell Us North to:

- Comply with the law in respect of the data it holds
- Follow good practice
- Protect Tell Us North's supporters, staff, volunteers and other individuals
- Protect Tell Us North from the consequences of a breach of its responsibilities
- Be open and honest with individuals whose data Tell Us North holds
- Provide training and support for Directors, Committee members, staff and volunteers who handle personal data, so that they can act confidently and consistently

2.1.1. Failure to follow this policy could result in:

- Damage to Tell Us North's reputation
- Individuals suffering embarrassment or inconvenience, or even real harm and distress
- A large monetary penalty imposed to Tell Us North by the Information Commissioner's Office

2.2. General Data Protection Regulation 2018

2.2.1 The regime for UK data protection is set out in the Data Protection Act 2018, along with the General Data Protection Regulation (GDPR). The GDPR regulates the processing of information relating to living and identifiable individuals (data subjects). This includes the obtaining, holding, using, or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

2.2.2. Data users must comply with the data protection principles of good practice which underpin the GDPR and best practice for information governance and data security and protection. As such personal data must be:

- Obtained and processed fairly and lawfully
- Held only for specified lawful purpose(s)
- Adequate, relevant, and not excessive in relation to the purpose(s) for which it is held
- Accurate and, where necessary, kept up to date
- Not kept longer than necessary
- Processed in accordance with GDPR
- Kept secure and protected
- Not transferred to countries without adequate data protection

2.3. Types of information covered by this policy

2.3.1 Tell Us North holds three types of information:

- Personal information: information held about individuals such as names, addresses, job titles
- Sensitive personal information: information held about individuals (for example employees and volunteers) such as with regard to health and disability

- Organisational information: publicly available information about organisations and some confidential information

2.3.2. This policy applies to information relating to identifiable individuals, even where it is technically outside the scope of the GDPR, by virtue of not meeting the strict definition of “data” in the GDPR.

2.3.3. Information about organisations is not covered by the GDPR. However, there is sometimes ambiguity about whether certain information is personal or organisational, for example the contact details for a small organisation might be someone’s home address or personal email address. Also Tell Us North strives for best practice. For these reasons organisational information is covered by this policy.

3. Key risks

3.1. Tell Us North has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately)
- Breach of security leading to unauthorised access
- Failure to establish efficient systems to manage and record changes, leading to personal data not being up-to-date
- The resulting negative consequences to individuals if personal data is not up-to-date or if inaccurate data has been recorded
- Insufficient clarity about the range of uses to which personal data will be put — leading to data subjects being insufficiently informed
- Failure to offer choice, where appropriate, to data subjects about how personal data is used
- Data protection issues in partnerships and other collaborative relationships
- Data protection issues in relation to contractors
- Data processor contracts

4. Responsibilities

4.1. Directors

4.1.1. The Board of Directors recognises its overall responsibility for ensuring that Tell Us North complies with its legal obligations.

4.2. Senior Information Risk Owner (SIRO)

4.2.1. The Senior Information Risk Owner is currently the Chief Executive, whose responsibilities include to:

- Brief the Board on data protection responsibilities
- Review data protection and related policies
- Advise other staff on data protection issues
- Ensure that data protection induction and training take place
- Register with (notify) the Information Commissioner’s Office
- Handle subject access requests
- Approve unusual or controversial disclosures of personal data
- Approve contracts with data processors
- Ensure systems are put in place to keep the ICT network secure

4.3. Data Protection Officer (DPO)

4.3.1. The Data Protection Officer is currently the Office manager, whose responsibilities include;

- to inform and advise Chief Executive and staff about obligations to comply with the UK GDPR and other data protection laws;
- to monitor compliance with the UK GDPR and other data protection laws, and with data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor, data protection impact assessments.
- to cooperate with the ICO
- to be the first point of contact for the ICO and for individuals whose data is processed (employees, public etc).

4.4. Staff and volunteers

4.4.1. All staff and volunteers are required to read, understand, and accept any policies and procedures that relate to the personal and organisational data they may handle in the course of their work.

4.5. Enforcement

4.5.1. Significant breaches of this policy will be handled under Tell Us North's Disciplinary Policy and Procedure.

5. Security

5.1. Scope

5.1.1. This section of the policy only addresses security issues relating to personal data.

5.2. Specific risks

5.2.1. Tell Us North has identified the following risks:

- The need to protect data while it is in transit
- The misuse of personal information by staff or volunteers with authorised access
- Unauthorised access to data by staff and volunteers while working, or no longer working, for Tell Us North
- Staff or volunteers being tricked into giving away information, especially over the phone
- Poor website security providing a means of access to personal contact details

5.3. Security measures

5.3.1. When in transit with sensitive and confidential records staff must:

- Make sure there is no other option available to them
- Never take the only copy with them if it is possible to make and retain a duplicate paper or electronic copy on the IT network. Staff must assess the impact of loss of the original and make a copy if that impact is unacceptable
- Only use password protected (encrypted) memory sticks for transferring electronic copies
- Take only as much as is necessary and only for as long as necessary
- Return it to its normally secure location as soon as possible
- Take all reasonable precautions to keep records safe and secure

5.3.2. If sensitive and confidential records are being sent by post then staff must send them by tracked and signed for postage e.g. Royal Mail Tracked.

5.3.3. Laptops are inherently insecure and so personal data should never be stored on them

5.3.4. Training is provided to reinforce the need for confidentiality and data protection

5.3.5. Access to data, information and files is defined by job role

5.3.6. Data is stored securely – paper copies are kept in a locked drawer or filing cabinet and a password is needed to access electronic copies

5.3.7. When staff and volunteers leave Tell Us North, their login/password details are removed from the ICT network

5.3.8. Staff and volunteers are only to share personal data on a need-to-know basis

5.3.9. Staff, volunteers, and directors working from home are never to store confidential information on their home computer

5.3.10. Staff and volunteers should not leave confidential information uncovered on a desk or displayed on a computer screen when away from the workstation. They must adhere to the clean desk and screen policy.

5.3.11. Paper copies of confidential data being handed to another member of staff or volunteer should be concealed in a folder or envelope marked “Confidential”

5.3.12. Due care and attention is taken when discussing or taking personal data details over the phone to ensure they cannot be overheard

5.3.13. Information about an individual will only be passed to another agency or to other persons outside of Tell Us North with the consent of the individual and where possible this will be with written consent, or if there is a legal basis to (see Section 5 – Confidentiality)

5.4. Backups

5.4.1. Data, information, and files saved on the ICT network is backed up to an onsite device hourly between 8am and 8pm every day, Monday to Friday. This equals approximately 12 backups per day. The backups are image-based backups which are encrypted to prevent unauthorised access and have a retention of up to 8 months. A copy of the backup data is uploaded and hosted offsite with the IT support provider. The onsite backup device allows for faster data restores when required and the offsite allows for data recovery in the event of an onsite disaster

6. Data recording and storage

6.1. The General Data Protection Regulation covers the processing of information relating to living and identifiable individuals (data subjects). This includes the obtaining, holding, using, or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

6.2. Accuracy

6.2.1. Tell Us North holds data in databases, and record and storage systems, to help it deliver its activities and manage the organisation. Tell Us North conducts annual reviews of records of processing to ensure data stored is in line with GDPR. Procedures for ensuring that records remain accurate and consistent and, in particular:

- ICT systems are designed, where possible, to encourage and facilitate the entry of accurate data
- Data on any individual is held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary additional data sets
- Effective procedures are in place so that all relevant systems are updated when information about any individual changes
- Staff or volunteers who need to keep more detailed information about individuals

6.3. Archiving

6.3.1. Archived paper records of personal data are securely stored in a locked drawer or filing cabinet.

6.4. Disposal

6.4.1. Paper copies of personal data are securely shredded, and electronic copies deleted once they have reached the end of the retention period.

7. Subject access requests

7.1. A subject access request is a written request made by, or on behalf of, an individual for information which they are entitled to ask for under the General Data Protection Regulation.

7.2. Under the right of subject access, an individual is entitled only to their own personal data, and not to information relating to other people (unless they are acting on behalf of that person). For information to be personal data, it must relate to a living individual who can be identified from that information.

7.3. Responsibility

7.3.1. All subject access requests will be handled by the Senior Information Risk Owner and must be responded to within one calendar month, starting from the day the request is received. If Tell Us North needs something from the individual to be able to deal with their request, for example ID documents, the time limit will begin on the day this is received.

7.3.2. If the request is complex or the individual makes more than one, the response time may be a maximum of three calendar months.

7.4. Procedure for making a request

7.4.1. Subject access requests must be made in writing. All staff and volunteers are required to pass on anything which might be a subject access request to the Senior Information Risk Owner without delay.

7.4.2. All those making a subject access request will be asked to identify any Tell Us North member of staff or volunteer who may also hold information about them, so that this data can be retrieved.

7.4.3. Tell Us North has a form to facilitate this process (see Appendix 1 – GDPR subject access request form) which is available on request. However, any subject access request submitted in writing (hard copy or email) must be accepted as a valid subject access request.

7.5. Provision for verifying identity

7.5.1. Where the individual (data subject) making a subject access request is not personally known to the Senior Information Risk Owner their identity must be verified before any information is handed over.

7.6. Charging a fee

7.6.1. This information will be provided free of charge. However, Tell Us North will charge a reasonable fee for the administrative costs of complying with a request if it is manifestly unfounded or excessive, particularly if repetitive requests are made.

7.7. Procedure for granting access

7.7.1. The requested information will be provided in writing, by letter or email as appropriate, unless the data subject has made a specific request to be given supervised access in person. It may not be possible to comply with the request if it would mean disclosing information about another individual who can be identified from that information.

7.8. Information Commissioner's Office: Right of access

7.8.1. For information about how to handle a subject access request, refer to the Information Commissioner's Office website.

8. Transparency

8.1. Tell Us North is committed to ensuring that in principle data subjects are aware that their data is being processed and:

- For what purpose it is being processed
- What types of disclosure are likely
- How long the information will be held for
- How to exercise their rights in relation to the data

8.2. Data subjects will generally be informed in the following ways:

- Staff: during induction
- Volunteers: in the volunteer application pack and during induction
- Directors: during their induction
- Job applicants: a statement about data protection is included in each application pack
- Tell Us North supporters and service users: when they sign up (on paper, online or by phone) for services or to purchase products

8.3. Standard statements are used on booking forms for Tell Us North events.

8.4. Whenever data is collected, the number of mandatory fields will be kept to a minimum and data subjects will be informed which fields are mandatory.

9. Consent

9.1. Underlying principles

9.1.1. Consent will not be sought for most processing of information about **staff**, with the following exceptions:

- Staff details will only be disclosed for purposes unrelated to their work (for example financial references) with their consent
- Staff working from home will be given the choice over what contact details, for example a phone number, will be made available to those persons needing to speak with them during their working day

9.1.2. Information about individuals involved in any activity (including photographs) will only be made public with their consent.

9.1.3. Personal data about service users will be held only with the knowledge and consent of the individual.

9.2. Opting out

9.2.1. A service user can request to opt out of their data being recorded, but this may affect the service Tell Us North can give them. The implications of opting out will be explained to any individual requesting this to enable them to make an informed decision.

9.3. Withdrawing consent

9.3.1. Tell Us North acknowledges that, once given, consent can be withdrawn, but not retrospectively. There may be occasions where Tell Us North has no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

10. Direct marketing

10.1. Underlying principles

10.1.1. Tell Us North does not send unsolicited marketing to private individuals. Tell Us North will treat the following direct communication with individuals as marketing:

- Seeking donations and other financial support
- Promoting any Tell Us North services
- Promoting events
- Promoting sponsored events and other fundraising exercises
- Marketing on behalf of any other external company, public body or voluntary organisation

10.2. Opting out

10.2.1. Whenever data is first collected which might be used for any marketing purpose, this purpose will be made clear, and the data subject will be given a clear opt out. If it is not possible to give a range of options, any opt-out which is exercised will apply to all Tell Us North marketing.

10.3. Electronic contact

10.3.1. Tell Us North will only carry out telephone or email marketing where consent has been given in advance for Tell Us North to use these forms of communication.

10.3.2. Whenever email addresses are collected, any future use for marketing will be identified, and the provision of the address made optional.

11. Staff training and acceptance of responsibilities

11.1. Induction

11.1.1. All Tell Us North directors and staff, as well as any volunteers who are to have access to any kind of personal data, will have their responsibilities outlined during their induction. They are also required to sign a statement indicating that they have been made aware of their responsibilities regarding confidentiality (see Confidentiality policy)

11.2. Training

11.2.1. Data protection and information governance will be included in further training for staff and volunteers.

11.3. Other related policies

11.3.1. The following policies will also be administered in line with this Data Protection Policy:

- Confidentiality Policy
- Records retention policy
- Data breach policy and procedure
- ICT Policy and Procedures
- Recruitment and Selection Policy and Procedure
- Whistleblowing Policy

12. Definition of terms

Data	Information held electronically or in hard copy formats (including photographs and video material).
Data Controller	The person or organisation legally responsible for complying with the Data Protection Act, i.e. responsible for why and how personal data is being stored and used.
Senior Information Risk Owner	The designated person within an organisation that collects personal data who is responsible for making sure that the organisation follows the requirements of the General Data Protection Regulation.
Data processor	An organisation or individual to whom data processing has been outsourced. When work is outsourced, which involves the contracting organisation having access to personal data, there must be a suitable written contract in place, paying particular attention to security. The Data Controller remains responsible for any breach of data protection brought about by a data processor.
Data subject	An individual about whom personal data is held.
Direct marketing	The communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.
Personal data	Information about a living individual who is identifiable from the data held on them by a Data Controller.
Privacy statement	Information for data subjects telling them in a clear and transparent way the legal basis for the Data Controller to hold their data, how long it will be used and how long it will be held.
Processing	Any use of personal data, including obtaining, storing, using, disclosing or destroying.
Record	A set of information about one individual.
Subject access	The right of an individual to have a copy of the information a Data Controller holds about them.
Third party	Term used to describe someone other than the data subject that the data is about.

Appendix 1 - GDPR subject access request form

Tell Us North use
Date received _____
Date completed _____
TUN staff _____

Tell Us North
General Data Protection Regulation subject access request form

Subject access request (2018 General Data Protection Regulation)

You are entitled to see most of the information we hold on you. If you wish to request a copy of any of this information, please complete this form and return it to Tell Us North, MEA House, Ellison Place, Newcastle upon Tyne, NE1 8XS. Alternatively, if you prefer not to use this form, please submit your request in writing to the same address or by emailing info@tellusnorth.org.uk

Name _____
Address _____
_____ Postcode _____
Telephone (optional) _____
Email address (optional) _____

Please tick if you have ever been a Tell Us North:

☐ employee ☐ volunteer ☐ client (or used our services)

If you have not ticked any of the above, please explain why you think we might hold information about you.

If we may have known you under a different name, what would it be?

Do you know of any Tell Us North staff members or volunteers that could hold personal information about you?

If you are requesting a copy of particular information (for example a certain type of record or emails between specific dates) what is that?

I wish to request a copy of the records you hold about me.

Signed _____ Date _____

Continued overleaf …

Please note

- We may need to ask you for additional means to confirm you are the person about whom you are requesting information.
- If you are not the data subject (the person the information is about), we will need evidence that you are authorised to act for that person.
- We will reply as quickly as we can. We aim to reply within three weeks, but we may take up to one month of receipt of your request. If you have asked for a copy of the information, we will send it to the address you have given above.
- We have information about staff, volunteers, clients and people we think might be interested in our work. We do not keep this information once we no longer need it, so if you were in touch with us some time ago we may no longer hold any information about you.
- We will provide the information you have requested, but please note that we may not be allowed to show you information which is also about, or which identifies, someone else.