New Galloway Community Enterprises Ltd

Data Protection Policy

1. Introduction

New Galloway Community Enterprises Ltd (NGCE) recognises that it stores and processes relatively large amounts of data during the course of its operation. This includes data on staff, Board members, shareholders, customers and suppliers. Staff, volunteers, shareholders, service users, customers and other people who work with us have a right to privacy and to expect that all personal information about them will be handled sensitively and confidentially. NGCE also has a legal responsibility under the General Data Protection Regulations (GDPR) that came into force in May 2018 to keep this data secure and private.

NGCE has undertaken an audit of all the personal data that it keeps, under three headings – Shop Operations, Community Engagement Worker and NGCE Ltd. 'Sensitive' personal data has been accorded particular priority. This audit has informed this Policy, an Action Plan and our Privacy Statements.

Most breaches in confidentiality happen through lack of thought or consideration of the possible consequences, or a lack of secure facilities, so all people involved with the storage and processing of NGCE data should familiarise themselves with this Policy and the compliance actions required.

Note that for the purposes of this Policy, 'staff' refers to the employees of NGCE Ltd, casual workers and volunteers in the shop, student placements or work experience positions, and any self-employed people working for NGCE Ltd.

2. Data Protection Principles

All data users must comply, be responsible for and be able to demonstrate compliance with the following Data Protection principles:

- Personal data must be processed fairly and lawfully and in a transparent manner in relation to individuals.
- Personal data must only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

- Personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Personal data must be 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measurers required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- Personal data shall be 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.
- Personal data shall not be transferred to another country without appropriate safeguards being in place;
- Personal Data shall be made available to Data Subjects, and Data Subjects allowed to exercise certain rights in relation to their Personal Data.

The Registrar can take enforcement action against a data user breaching the principles, who can in turn appeal to an independent Data Protection Tribunal. If the tribunal upholds the Registrar's enforcement action, failure to comply becomes a criminal offence.

Any breach in the policy could have very serious consequences for an individual or for the association and will be treated as a serious disciplinary matter.

3. Sensitive Personal Data

Although all Personal data is covered by this Policy, Sensitive Personal data requires even more care in handling. Examples of this type of data are:

- Race
- Ethnic origin
- Politics
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sexual orientation

4. Lawful bases

The GDPR regulations set out the only conditions under which data can be stored or processed. These are:

- **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law.
- **Vital interests:** the processing is necessary to protect someone's life.
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

5. Policy

NGCE Ltd, its staff and Board members will:

- Treat all personal and sensitive data as confidential.
- Comply with the law regarding the storage and processing of information.
- Not disclose personal information without the prior informed consent of the individual concerned.
- Not gain or attempt to gain access to information they are not authorised to have.

Specifically, NGCE will:

- Only keep such data as is required for legal compliance or operation of its business.
- Train staff and Board members in the safe and secure processing of this data.
- Ensure that a Board member is appointed single point of responsibility for data protection.
- Be clear on the legal basis under which each element of data is stored and processed.
- Keep copies of consent forms if data is being collected under a Consent basis.
- Tell people how we manage their data through Privacy Statements.
- Store such data in secure electronic or paper filing systems.
- Delete data as it becomes out of date, no longer needed or is requested to be deleted.
- Have a process in place to respond to requests to see personal data.
- Audit their data storage and processing processes annually.

Privacy Statements will be created and published for:

- Users of the Community Engagement Worker's services.
- Staff
- Shareholders

6. Procedures

6.1 Storage of Data

Personal Data must not be kept in an identifiable form for longer than is necessary for the legitimate business purpose or purposes **for which it was originally**

collected, including for the purpose of satisfying any legal, reporting or safeguarding requirements.
Regular audits will ensure that Personal Data is deleted at the appropriate time. Paper Personal Data will be destroyed or shredded; electronic data will be deleted from databases.

6.1.1 Electronic data.

- Electronic personal data should be contained only in the databases identified at audit, and should be stored within a GDPR-compliant system.
- All personal laptops should be password protected and kept locked when not in use.
- All personal laptops should be securely filed away at the end of a working day.
- Database information should be stored in such a way that if a Data Subject requests information about them, the request can be fulfilled promptly and accurately.

6.1.2 Paper data

- Paper files should be stored within locked filing cabinets, with the keys not available to the public.
- All filing cabinets should be locked at the end of each working session.
- Paper files should not be left in the open where non-authorised people can view them.

6.1.3 Sensitive personal data

Sensitive personal data (whether electronic or paper) should be treated as above, with the additional proviso that:

- Files must be stored in separate areas where access is given to only named individuals e.g. a separate area of the server, or a separately locked filing cabinet.

6.2 Obtaining consent

One of the lawful bases for storing and processing data is Consent. If this basis is being used, the Consent Form must list this information:

- Where the information is being stored (e.g. locked filing cabinet; password protected server system)
- How long the information will be stored for
- That the subject has the right to request that the information be erased.
- Who the information will be shared with.

6.3 Breaches

Data breaches involving personal data must be reported to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. This is unless an organisation can prove that a personal data breach has little to no risk of impacting on an individual's rights. A decision not to report a breach must be able to be justified, so must always be formally documented.

Breaches can be reported to the ICO on 0303 123 1113 or by completing a security breach notification form on www.ico.org.uk. The ICO website gives details as to what information is required to be reported at this point.

If a breach is likely to impact significantly on an individual's rights or freedoms, then the individual must also be informed about the breach.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
Personal data breaches can include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

6.4 Subject Access Requests

An individual who makes a written subject access request is entitled to be:

- Told whether NGCE Ltd holds any personal data about them
- Supplied with a copy of all the personal information held about them (unless the information is covered by an exemption).

Individuals must be told which databases of information NGCE holds and must request information specifically per database. Personal information from **only** the databases requested must be given out.

- A response is required within one month of receiving the request.
- Information must be supplied in a form that is in a commonly used electronic format, and apart from routine amendment, must not be specially amended to make it acceptable to the data subject.
- No charge can be made for fulfilling the access request.
- Failure to respond to a request is not a criminal offence, but subjects are entitled to complain to the Registrar for a court order for access.

The GDPR does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, NGCE will need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney.
If NGCE is unable to clarify or receive confirmation that authority has been given to a third party it may send the response directly to the individual and they may then

choose to share the information with the third party after having had a chance to review it.

If any individual wishes to request a copy of the data held on them by the NGCE Ltd, then they must complete a Subject Access Request form (to be held on the website) and then submit it to the Chair of the Board who will ensure that the request is dealt with.

6.5 Audits

NGCE will carry out yearly audits of its data storage and processing operations, split into areas of operation as appropriate. The actions generated by these audits will be added to the NGCE Risk Register and monitored for timely completion at Board level.

These audits also form the GDPR records of our data processing activities and must therefore be kept up to date at all times if additional data is stored or processes, or if the methods of storage and processing change.

7. Data Protection Officer

A named Board member will be designated with responsibility for Data Protection and will have responsibility for ensuring that this Policy is being adhered to, through a system of spot checks and regular audits.

8. Training

All existing staff and Board members will be trained in this Policy and its implementation after adoption by the Board.
New staff and Board members will have the key points from the Policy included in their Induction process.
This Policy will be included in the Staff handbook, and all staff and Board members will be encouraged to familiarise themselves with it routinely, as with all policies.

9. Contravention of this policy

Failure to comply with any of the requirements of this policy is a disciplinary offence and may result in disciplinary action being taken under New Galloway Community Enterprises disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal or the termination of the casual work, volunteering or work experience placement agreement.

Considered and adopted by the Board of NGCE Ltd, 24 May 2018