Data Protection Policy

Data Protection: Introduction

Gateway into the Community is a charity that supports people with learning disabilities. We collect and use information about people with whom we work. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means.

We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we deal. We will ensure that we treat personal information lawfully and correctly.

To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).

This policy sets out Gateway into the Community's procedures for the collection, storage, use and sharing of personal data and data for electronic communication between organisations. It also covers our response to any data breach and other rights under the GDPR.

The Policy will be reviewed by the trustees of Gateway into the Community every three years, or earlier if there are changes to legislation and/or to the charity's use of data . Current relevant legislation is: the Data Protection Acts 1994 and 1998, the General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR).

What data is relevant?

Data Protection legislation is concerned with the use of personal data, held on electronic systems, in paper filing and online identifiers such as location data and cookies.

Personal data is defined by the Information Commissioners Office (ICO) as data that relates to a living individual who can be identified

- from that data, or
- from that data and other information in the possession of (or likely to come into the possession of) the data controller e.g: expressions of opinion about an individual, or
- from codified records that do not identify individuals by name but, for example, bear unique reference numbers that can be used to identify the individuals concerned.

Special categories of personal data means information that could be used in a discriminatory way, so needs to be treated with greater care than other personal data, i.e: information about:

- race or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature

- trade union membership
- physical or mental health or condition
- sex life
- sexual orientation
- genetic and biometric data

Criminal offence data is data which relates to an individual's criminal convictions and offences or related security measures:

- commission or alleged commission by the data subject of any offence
- any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.

Definitions

A data subject: Anyone whose data is processed.

A data controller: The organisation/ person who decides how and personal data is/will be, processed. Data controllers will usually be organisations, but can be individuals, for example self-employed consultants.

A data processor: Any person (other than an employee of the data controller) who processes the data on behalf of the data controller, eg: external payroll service providers.

Data processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection Principles

Under GDPR, all personal data obtained and held by Gateway into the Community must be processed according to a set of core principles. We will ensure that:

- processing will be fair, lawful and transparent
- personal data will be collected for specific, explicit, and legitimate purposes and will not be further processed in any manner incompatible with those purposes
- personal data collected will be adequate, relevant and limited to what is necessary for the purpose(s) for which they are processed
- personal data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- personal data will not kept for longer than is necessary for its given purpose
- appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction of or damage to, data
- we will comply with the relevant GDPR procedures for international transferring of personal data

Who do we collect/process/store data from?

- **Members of Gateway into the Community:** current, past and potential – this will be personal data and will include special category data

- **Employees, trustees and volunteers:** current and former – this will be personal data and may include special category data
- **Job applicants:** this will be personal data
- **Other organisations with which we work:** this is unlikely to be personal data but it can be in some cases for example where email addresses identify an individual

More information about our data processing activities is included in our **Privacy Notices for Members, Employees, Volunteers, Trustees and Job Applicants**

Rights of data subjects

Under GDPR, all data subjects have the following rights:

- the right to be informed about the data we hold and what we do with it;
- the right of access to the data we hold – see Access to Data below;
- the right for any inaccuracies in the data we hold, however they come to light, to be corrected - also known as 'rectification';
- the right to have data deleted in certain circumstances - also known as 'erasure';
- the right to restrict the processing of the data;
- the right to transfer the data we hold to another party. This is also known as 'portability';
- the right to object to the inclusion of any information;
- the right to regulate any automated decision-making and profiling of personal data.

More information can be found on each of these rights in our **Privacy Notices**.

Responsibilities of data controller

In order to protect personal data, all within Gateway into the Community who must process data as part of their role have been made aware of our policies on data protection and have received appropriate training. The importance of confidentiality is emphasised during the induction process for staff and volunteers including trustees and all are required to sign a confidentiality agreement.

Lawful bases of processing

Gateway into the Community acknowledges that processing of personal data may be only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis to each processing activity.

Where no other lawful basis applies, we may seek to rely on the data subject's consent in order to process data.

However, we recognise the high standard attached to the use of consent which must be:

- freely given – consent will not be valid if the data subject does not have a genuine and free choice or cannot refuse or withdraw consent without detriment
- specific to the purpose for which the data is being used
- informed and unambiguous
- active not implied – silence is not consent; pre-ticked boxes, inactivity, failure to opt out or passive acquiescence will not constitute valid consent

Ways in which we may ask for consent include:-

- Written consent;
- Ticking a box on a web page;
- Choosing technical settings in an app;
- Verbal consent (which is then recorded in writing)
- Any other statement/conduct that clearly indicates the data subject's acceptance of the proposed processing of personal data, for example cookie acceptance.

In line with PECR we will not contact individuals for direct marketing or fundraising purposes by email, the internet, phone, fax or any new electronic systems that may be introduced without prior consent. (NB: Business to business communications to generic addresses such as “admin@” “info@” do not require consent.)

All Gateway into the Community’s mailings make it clear who the sender is, so the recipient’s ability to opt out is viable.

Our website makes it clear we use cookies to collect details of visitors to our website and gives them an opportunity to refuse their operation.

Access to data

To exercise their right to access the personal data that we hold on them, data subjects should make a Subject Access Request. Gateway into the Community will comply with the request without delay, and within one month, unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.

No charge will be made for complying with a request unless the request is clearly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the data subject making the request. In these circumstances, a reasonable charge will be applied.

Data disclosures

Gateway into the Community may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- for the purposes of preventing or detecting crime;
- required by a rule of law or by the order of a court or tribunal;
- to assess or collect any tax or duty
- in the particular circumstances justified as being in the public interest;
- disabled employees - whether reasonable adjustments are required to assist them at work;
- individuals’ health data - to comply with health and safety or occupational health obligations towards the data subject
- to report a safeguarding risk or emergencies such as a health crisis
- data disclosed to parents/carers in respect of a member’s health, safety and welfare
- member data disclosed to authorised recipients in relation to education and training

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data security

We keep several categories of personal data on members, employees, volunteers including trustees and job applicants in order to carry out effective and efficient processes. We keep

this data in a personnel file relating to each individual and we also hold the data within our IT systems, which may include our email system.

Hard copy personal information is kept in a locked filing cabinet or safe in the Gateway into the Community office, which is itself locked outside office hours.

Where data is computerised, it is encrypted or password protected both on local hard drives and on a network drive that is regularly backed up. If a copy is kept on removable storage media, those media themselves are kept in a locked filing cabinet or safe. Employees whose role involves the processing of personal data have been trained in ensuring data is processed in line with GDPR and are aware of their responsibilities.

All employees of Gateway into the Community are instructed to store files or written information of a confidential nature in a secure manner so that the information is only accessed by people who have a need and a right to access it. Employees must always use the passwords provided to access the charity's computer system and not abuse them by passing them on to people who should not have them. Screen locks must be implemented on all PCs, laptops etc when unattended and employees must ensure that laptops or USB drives are not left where they can be stolen. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Data should not be kept or transported on individual employees' personal laptops, USB sticks, or similar devices, unless prior authorisation has been received and only where absolutely necessary. In normal circumstances, the charity's devices must always be used.

Failure to follow Gateway into the Community's rules on data security may be dealt with via the charity's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

Third party processing

Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes appropriate technical and organisational measures to maintain Gateway into the Community's commitment to protecting data.

Requirement to notify breaches

All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

Training

New employees and volunteers including trustees must read and understand the policies on data protection and confidentiality as part of their induction and must sign a confidentiality agreement. All employees receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

Those employees who need to use the charity's IT systems are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the charity of any potential lapses and breaches of the charity's policies and procedures.

Records

Gateway into the Community keeps records of its data processing activities including the purpose for the processing and retention periods. These records will be kept up to date so that they reflect current processing activities.

Data protection compliance

Gateway into the Community does not need a designated Data Protection Officer under the GDPR. However, our appointed compliance officer in respect of our data protection activities is:

Gabby Keaveny
Administrator
Gateway into the Community
3 St Mary's Wynd
Hexham
NE46 1LW

December 2020