Charity number 1197599

GDPR and Data Collection Policy for Brereton Big Local CIO

Aims and scope of this policy.

"At Brereton Big Local CIO, we are committed to maintaining the trust and confidence of our visitors to our web site. We want you to know that Brereton Big Local CIO is not in the business of selling, renting, or trading email lists with other companies and businesses for marketing purposes. We just don't do that sort of thing. But just in case you don't believe us, in this Privacy Policy, we've provided lots of detailed information on when and why we collect your personal information, how we use it, the limited conditions under which we may disclose it to others and how we keep it secure. Grab a cuppa and read on."

Brereton Big Local CIO values the data we collect not only to keep you in the loop of what we are up to and to let you know whether we need your help or your advice, but also for our very important consultations which keep our Million pound spend and volunteer work moving. Your data is stored safe on our Web email system, photos are displayed on advertising printed work where permissions have been given or any printed photos are locked in file cabinets and only used for display boards.

This Policy details all this information in more detail.

Mailing Lists
As part of our consultation process, we collect personal information. We use that information for a couple of reasons: to tell you about stuff you've asked us to tell you about; to contact you if we need to obtain or provide additional information; to check our records are right and to check every now and then that you're happy and satisfied, and for further consultation. We don't rent or trade email lists with other organisations and businesses. We use a third-party provider, MailChimp, to deliver our updates.

For more information, please see MailChimp's privacy notice. You can unsubscribe to general mailings at any time of the day or night by clicking the unsubscribe link at the bottom of any of our emails or by emailing our Support Worker sue.biglocal@gmail.com .

Ticketing Data

"When you purchase a ticket, we collect personal information. We use that information for a couple of reasons: to tell you about stuff you've asked us to tell you about; to contact you if we need to obtain or provide additional information; to check our records are right and to check every now and then that you're happy and satisfied, and for further consultation. We don't rent or trade email lists with other organisations and businesses"
We use a third-party provider, MailChimp, to deliver our updates. For more information, please see *MailChimp's privacy notice*. You can unsubscribe to general mailings at any time of the day or night by clicking the unsubscribe link at the bottom of any of our emails or by emailing our Support Worker *sue.biglocal@gmail.com* .

We use Eventbrite to deliver our ticket sales. For more information, please see https://www.eventbrite.co.uk/support/articles/en_US/Troubleshooting/eventbrite-privacy-policy?lg=en_GB.

Photos

Photo permission is taken as granted unless otherwise stated; this will give us the permission within our publicity material. Once this has been publicised this information cannot be changed, if you feel the need to discuss this prior to giving consent then please discuss this with a member of the Brereton Big Local CIO team who is taking your photograph or email sue.biglocal@gmail.com.

Access to your personal information

Under GDPR, anyone has the right to access and amend any of his or her personal data that we hold.
You are entitled to view, amend, or delete the personal information that we hold. Email your request to our Support Worker Sue at sue.biglocal@gmail.com

Changes to this Privacy Notice

This Policy was created November 2022 and will be monitored/reviewed over the next 12 months to make sure it is in line with the GDPR rulings

This policy applies to the processing of personal data in manual and electronic records kept by the CIO in connection with its human resources function as described below. It also covers the CIO's response to any data breach and other rights under the General Data Protection Regulation and current Data Protection Act.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers, and self-employed contractors. These are referred to in this policy as relevant individuals.

The lead trustee for data protection is Karen Mann to whom any concerns about the operation of this policy should be referred.

Definitions

"Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

"Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

"Criminal offence data" is data which relates to an individual's criminal convictions and offences.

"Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether 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.

Our commitment

The CIO makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of the CIO, the CIO will ensure that the third party takes such measures to maintain the CIO's commitment to protecting data. In line with current data protection legislation, the CIO understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

Types of data held

Personal data is kept in personnel files or within the CIO's HR systems. The following types of data may be held by the CIO, as appropriate, on relevant individuals:

- name, address, phone numbers - for individual and next of kin
- CVs and other information gathered during recruitment.
- references from former employers
- National Insurance numbers
- job title, job descriptions and pay grades.
- conduct issues such as letters of concern, disciplinary proceedings.
- holiday records
- internal performance information
- medical or health information
- sickness absence records
- tax codes
- terms and conditions of employment
- training details.

Relevant individuals should refer to the CIO's privacy notice for more information on the reasons for its processing activities, the lawful bases it relies on for the processing and data retention periods.

Data protection principles

All personal data obtained and held by the CIO will:

- be processed fairly, lawfully and in a transparent manner.
- be collected for specific, explicit, and legitimate purposes.
- be adequate, relevant, and limited to what is necessary for the purposes of processing.
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay.
- not be kept for longer than is necessary for its given purpose.
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction, or damage by using appropriate technical or organisation measures.
- comply with the relevant data protection procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed.
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)

- the right to restrict the processing of the data.
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

Procedures

The C IO has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

- it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way.
- it provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially.
- it can account for all personal data it holds, where it comes from, who it is shared with and who it might be shared with
- it carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by the CIO.
- it recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing, and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. The CIO understands that consent must be freely given, specific, informed, and unambiguous. The CIO will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time.
- it has the appropriate mechanisms for detecting, reporting, and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner and is aware of the possible consequences.
- it is aware of the implications international transfer of personal data internationally.

Access to data

Relevant individuals have a right to be informed whether the CIO processes personal data relating to them and to access the data that the CIO holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- a form on which to make a subject access request is available from your line manager. The request should be made to your line manager.
- the CIO will not charge for the supply of data unless the request is manifestly unfounded, excessive, or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request.
- the CIO will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

Relevant individuals must inform the CIO immediately if they believe that the data is inaccurate, either because of a subject access request or otherwise. The CIO will take immediate steps to rectify the information.

Data disclosures

The CIO may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties.
- disabled individuals - whether any reasonable adjustments are required to assist them at work.
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee.
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job.
- the smooth operation of any employee insurance policies or pension plans.

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

Data security

The CIO adopts procedures designed to maintain the security of data when it is stored and transported.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them.
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people.
- refrain from sending emails containing sensitive work-related information to their personal email address.
- check regularly on the accuracy of data being entered into computers.
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them; and
- use computer screen blanking to ensure that personal data is not left on screen when not in use.
-

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised the community support worker Support Worker Sue at sue.biglocal@gmail.com
Where personal data is recorded on any such device it should be protected by:
ensuring that data is recorded on such devices only where necessary.
using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted; and
ensuring that laptops or USB drives are not left lying around where they can be stolen.
Failure to follow the CIO's rules on data security may be dealt with via the CIO's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

International data transfers

The CIO does not transfer personal data to any recipients outside of the EEA.

Breach notification

Where a data breach is likely to result in a risk to the rights and freedoms of individuals, it will be reported to the Information Commissioner within 72 hours of the CIO becoming aware of it and may be reported in more than one instalment.

Individuals will be informed directly if the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, the CIO will do so without undue delay.

Training

New employees must read and understand the policies on data protection as part of their induction.

All employees will receive training covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach.

The nominated data controller/auditors/protection officers for the CIO are trained appropriately in their roles under data protection legislation.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and the CIO of any potential lapses and breaches of the C IO's policies and procedures.

Records

The CIO keeps records of its processing activities including the purpose for the processing and retention periods in its HR data record. These records will be kept up to date so that they reflect current processing activities.

To be reviewed and signed at the next AGM.

Signed & Agreed by all Trustees on date:	Policy version:	Review Date:
	V.1 11-22	11/2023