DATA PROTECTION POLICY

How to ensure that we treat personal information lawfully and correctly

Contents

DATA PROTECTION POLICY

INTRODUCTION

We may have to 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 carry out business. 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 applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources and service delivery functions. This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. It also applies to our clients, clients' families, and our supporters, commissioners and donors. These are referred to in this policy as relevant individuals. It also covers our response to any data breach and other rights under the GDPR.

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 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 us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:

- processing will be fair, lawful and transparent
- data be collected for specific, explicit, and legitimate purposes
- data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
- data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
- data is not kept for longer than is necessary for its given purpose
- data will 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
- we will comply with the relevant GDPR procedures for international transferring of personal data

TYPES OF EMPLOYEE DATA HELD

We keep several categories of personal data in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data:

- personal details such as name, address, phone numbers
- information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc
- details relating to pay administration such as National Insurance numbers, bank account details and tax codes
- medical or health information
- information relating to your employment with us, including:
- job title and job descriptions
- your salary
- your wider terms and conditions of employment

- details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information
- internal and external training modules undertaken

All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice for employees, which is available from your manager.

TYPES OF VOLUNTEER/CLIENT DATA HELD

We keep several categories of personal data to carry out effective and efficient processes. We collect this either in paper form or by electronic means, although it could be provided verbally. This information enables us to communicate to handle emergencies, respond appropriately to requests made to BCS or to report on aspects of our service delivery, including to our funders where appropriate. The information kept may include but it not limited to:

- records maintenance
- health and safety obligations
- identifying volunteering and training opportunities
- reregistration
- communication about your volunteering role

BCS uses the health data you provide:

- to keep you and others safe while volunteering
- in risk assessments, and to put in place countermeasures for identified risks

RIGHTS

Employees, volunteers and other users of BCS's services have the following rights in relation to the personal data we hold on them:

- the right to be informed about the data we hold on you and what we do with it;
- the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests".
- the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification'.
- the right to have data deleted in certain circumstances. This is also known as 'erasure' (also known as "right to be forgotten").
- the right to restrict the processing of the data.

- the right to transfer the data we hold on you 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.

RESPONSIBILITIES

In order to protect the personal data of relevant individuals, those within our business who must process data as part of their role have been made aware of our policies on data protection.

We have also appointed representatives with responsibility for reviewing and auditing our data protection systems.

LAWFUL BASES OF PROCESSING

We acknowledge that processing may only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.

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

However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. Subjects will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

ACCESS TO DATA

As stated above, individuals have a right to access the personal data that we hold on them. To exercise this right, individuals should make a Subject Access Request. We 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 manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the person making the request. In these circumstances, a reasonable charge will be applied.

Further information on making a subject access request is contained in our Subject Access Request policy.

DATA DISCLOSURES

The Charity 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.

- individuals with a disability or health condition - 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 or client.
- 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.
- to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.

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

We may also need to share certain data/information with third parties or statutory organisations for the purposes of safeguarding clients or individuals who have been harmed or are at risk of harm or abuse. More information can be found in our Safeguarding Policy and Procedure.

DATA SECURITY

All our employees are aware that hard copy personal information will be kept in a locked filing cabinet, drawer, or safe.

Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so that are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.

Where data is computerised, it is coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

Employees must 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.

Personal data relating to individuals should not be kept or transported on laptops, USB sticks, or similar devices.

Failure to follow the Charity'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 such measures to maintain the Charity's commitment to protecting data.

INTERNATIONAL DATA TRANSFERS

The Charity may be required to transfer personal data to a country/countries outside of the EEA. Transfers may take place because the Charity may use offsite IT systems that are provided by a cloud-based provider. Where this occurs, we will ensure that there are contractual terms in place to ensure data security. Data security will be the highest priority when identifying new IT service providers.

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

All employees 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 Charity are trained appropriately in their roles under the GDPR.

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 Charity of any potential lapses and breaches of the Charity's policies and procedures.

RECORDS

The Charity 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.

BCS keeps personal data for:

- 2 years after your volunteering role ends
- 2 years after you stop being a beneficiary of our services
- 7 years if your personal data relates to a formal complaint or a reported health and safety incident

DATA PROTECTION COMPLIANCE

Our appointed compliance officer/Trustee in respect of our data protection activities is: Tony Dawes

Day to day responsibility is: Volunteer Coordinator

DATA PROTECTION ACT: Information management protocol for data held on clients:

Volunteers, staff and Trustees of BCS use a variety of communication methods to share the personal information of clients that is necessary for the proper and safe running of the service. This includes WhatsApp groups used by Telephone Coordinators and another for Delivery Volunteers and Coordinators, using personal phone numbers. Additionally, Call Handlers and Coordinators email each other using personal email accounts. To ensure all data is used within the bounds of this Policy, all personnel will comply by the following:

BCS WhatsApp groups will be set by the group administrator to 'Disappear Messages After 90 Days'. The administrator will remove any and all group members who are no longer engaged in the proper function of that group for whatever reason. For example, a person is no longer active as a volunteer.
It is recommended that WhatsApp direct messages sent between personnel and received using personal phones should likewise be set to 'Disappear Messages After 90 Days.' However, it is recognised that people might also use WhatsApp for personal information exchange that does not fall within the scope of this Policy, for example where two volunteers share a friendship. In such cases, every month, each volunteer must check personal WhatsApp chats and delete BCS person identifiable information.

Every month, Call Handlers and Coordinators will check emails in their personal account for all sent and received correspondence that contains information falling within this Policy. Volunteers will delete all such emails unless they relate to active, current concerns about clients.

BUNGAY COMMUNITY SUPPORT:
DATA PROTECTION ACT: VOLUNTEER CONSENT

Registered Charity No: 1200141
Reg in Eng. & Wales/Scotland

In order to provide a professional and effective service, we need to keep a record of your personal information which may contain personal and sensitive information. To comply with the General Data Protection Regulations, we must tell you how this data will be used and ask for your permission. By signing this form, you are permitting Bungay Community Support (BCS), as Data Controller, to process your data for the purposes below. Permission to store your data.

This information will include your full name, contact details, the person to contact in event of emergency and details of your volunteering with us. In addition, we will use your contact details to keep you up to date with activities, training and special events.
All personal information is treated as private and confidential. This data will be stored in an electronic data base and the paper copies will be securely stored in a locked filing cabinet.

You have the right to see any information that we hold about you, and to have your details removed. We do not share your information with any other agencies or companies. Should you require us to provide a reference for you with an agency, then we would require you to give us written permission to do so. When you no longer volunteer at the foodbank, you may ask us to hold your personal information should you want to volunteer again at a later stage? If this is not the case, we will remove you from our data base and either return all paper copies to you or shred them whichever is your wish.

Consent:

I have read and understood the information above, and I give written consent for Bungay Community Support (BCS) to hold personal information about me.

I give my consent for Bungay Community Support (BCS) holding personal information for the purpose of receiving a paper/electronic communication.

Name	
Signature	
Date	
Email	

GDPR-Compliant Photo Consent Form

Name	
First Name	Last Name
Consenting Age	
The person in the image is of legal age	The person in the image is of below legal age

I hereby give my consent to Bungay Community Support (BCS) for the use of images where the person named is included therein, taken by said group for production and use which the named person may appear in websites owned by the BCS, publications produced, print advertisements introduced by them.

In giving this consent, I understand and declare that:

- I am giving this consent in my own free will, and not under duress or in any form of threat;
- That the images containing the person in this consent shall be held by BCS in accordance and compliance with the GDPR guidelines (the General Data Protection Regulation);
- That my information herein, as well as the images to be shared to the recipient shall not be disclosed to any other party without my written consent;
- That I hereby allow the use of images where the Subject is included shall belong to BCS for their own legitimate use for publicity purposes;
- I hereby agree to waive my rights to any claims to whatever BCS may use of the image;
- I may exercise my right to withdraw the use of my image anytime after from the effectivity of this consent in writing. After which, I am given the right to ask to cease the use of my images thereafter.
- By submitting this form with my signature below, I am affirming to the provisions mentioned above and the effectivity of this agreement shall commence.

Signature:**…….**

Signature of Legal Guardian (where person is under legal age at time of signing):

……

Date:……