Bullingdon Community Association

Data Protection Policy

Introduction

Bullingdon CIO is fully committed to compliance with the requirements of the Global Data Protection Regulation (GDPR) EU regulation 2016/679 from its implementation on 25th May 2018.

We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations. The legal basis of processing this data is legitimate interests. We recognise the importance of correct and lawful treatment of personal data as it helps to maintain confidence in our organisation and to ensure efficient and successful outcomes when using this data.

The types of personal data that we may process include information about current, past and prospective employees; community centre users, suppliers and other organisations with whom we have dealings.

Personal data may consist of data kept on paper, computer or other electronic media; all of which is protected under the GDPR.

Principles

We endorse and adhere to the six principles of the GDPR which are summarised as follows:

Data must:

1. be processed lawfully, fairly and in a transparent manner in relation to individuals
2. be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
3. be adequate, relevant limited to what is necessary in relation to the purposes for which they are processed
4. 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
5. 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 measures required by the GDPR in order to safeguard the rights and freedoms of individuals
6. 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

These principles apply to obtaining, handling, processing, transportation and storage of personal data.

Employees and agents of Bullingdon CIO who obtain, handle, process, transport and store personal data as part of their role must adhere to these principles at all times.

Handling of personal and/or sensitive information

Bullingdon CIO will, through appropriate management and the use of strict criteria and controls:

- observe fully the conditions concerning the fair collection and use of personal information
- specify the purpose for which information is used and the legal basis for its processing
- collect and process information only to the extent that it is needed to fulfil operational needs or legal requirements in line with the legal basis for processing specified
- endeavour always to ensure the quality of information used
- not keep information for longer than required, operationally or legally (see the data and record retention policy)
- to safeguard personal information by physical and technical means
- ensure that personal information is not transferred outside the EU without suitable safeguards
- ensure that the lawful rights of people about whom the information is held can be fully exercised

In addition, we will ensure that:

- there is someone with specific responsibility for data protection in the organisation (the Data Protection Officer (DPO)) - currently Trustee Tom Cook
- all staff managing and handling personal information understand that they are contractually responsible for following good data protection practice
- all staff managing and handling personal information are appropriately trained to do so - any data sharing is carried out under a written agreement, setting out the scope and limits of the sharing
- any disclosure of personal data will be in compliance with approved procedures

Individual rights

All individuals who are the subject of personal data hold the following rights under GDPR:

- to be informed about how the data will be used
- to access their data that is held
- to rectify their data if it is incomplete or inaccurate
- to erasure if there is no compelling reason for its continued processing
- to restrict processing
- to data portability, allowing individuals to obtain and reuse their data across different services
- to object to processing based on legitimate interests, direct marketing or processing for scientific, historical, statistical or public interest purposes
- to restrict automated decision making and profiling with their data

These rights are subject to certain exemptions which are set out in the GDPR. Any person who wishes to exercise any of these rights should make a request in writing to the DPO.

Any request for access will be provided free of charge unless it is deemed to be “unfounded or excessive” in which instance a reasonable fee may be levied. Multiple requests may also be subject to a reasonable fee at BCA’s discretion. If personal details are inaccurate, they will

be amended upon request. If by providing this information we would have to disclose information relating to or identifying a third party, we will only do so provided the third party gives consent, otherwise we may edit the data to remove the identity of the third party.

Personal information will only be released to the individual to whom it relates. The disclosure of such information to anyone else without their consent may be a criminal offence. Any employee who is in doubt regarding a subject access request should check with the DPO. Information must under no circumstances be sent outside of the EU without the prior permission of the DPO.

We will comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 1 month of receipt of a written request unless there is valid reason for delay. Valid reasons include, but are not limited to, complex and numerous requests. In such cases, the reason for delay will be explained in writing, within 1 month of receipt of the request, to the individual making the request.

Employee responsibilities

All employees must ensure that, in carrying out their duties, BCA is able to comply with its obligations under the GDPR. In addition, each employee is responsible for:

- checking that any personal data that he/she provides to us is accurate and up to date
- informing us of any changes to information previously provided, e.g. change of address
- checking any information that we may send out from time to time, giving details of information that is being kept and processed if, as part of their responsibilities, employees collect information about other people or about other employees they must comply with this policy. This includes ensuring the information is processed in accordance with the GDPR, is only processed for the purposes for which it is held under the legal basis of processing, is kept secure, and is not kept any longer than is necessary in line with the data and record retention policy

Employees are reminded that the GDPR does not just apply to records held relating to our employees, but also to any Centre Users files and/or records. Information stored on Centre Users should be reviewed regularly to ensure it is accurate and up to date. All documents, whether hand written or stored in emails (current or deleted) are potentially disclosable in the event of a request from an employee or client.

Data security and breaches

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted.

All staff are responsible for ensuring that any personal data which they hold is kept securely and that personal information is not disclosed either orally, in printed form, hand-written, electronically or otherwise to any unauthorised third party.

If any breach of personal data is detected, the data controller will be notified and steps taken to investigate and report on this to the management committee. If the breach is determined to have the potential to affect individuals' rights and freedoms the individuals affected, and any relevant supervisory body, must be notified as soon as possible and no later than within 72 hours.

Subject consent

Our contracts of employment require the consent of employees to the processing of personal data for the purposes of administering, managing and employing our staff. This includes: payroll,

benefits, medical records, absence records, sick leave, pay information, performance reviews, disciplinary and grievance matters, pension provision, recruitment, family policies (maternity, paternity, adoption etc.) and equal opportunity monitoring.

Information about an individual will only be kept for the purpose for which it was originally given.

Data relating to children

The GDPR imposes special regulation on the processing and storing of data relating to children. This includes a requirement that the privacy notice be written suitably simple enough that a child would understand. WOCA currently does not store or process data related to children. In future, if this changes, this policy will be revised in the first instance to reflect the processes around data associated with children.

Retention and disposal of data

Information will be kept in line with our document retention guidelines, as detailed in the data and record retention policy. All employees are responsible for ensuring that information is not kept in breach of the policy.

Documents containing any personal information will be disposed of securely, and paper copies will be shredded.

Implementation, monitoring and review of this policy

This policy, along with the data and record retention policy, will take effect from and replace the existing policies.

The policies will be subject to continuous monitoring by the Secretary and the DPO who will bring any developments or required changes to the attention of the management committee. They are subject to a triennial review by the management committee.

Approved by Management Committee July 2022