BEXLEY MOORINGS PROJECT

GENERAL DATA PROTECTION

REGULATION POLICY

The purpose of this policy is to set out how the requirements of Regulation (EU) 2016/679 (more commonly known as the General Data Protection Regulation ("**GDPR**") will be implemented and complied with.

From 25 May 2018, the GDPR (and any UK national law seeking to implement its provisions) regulates the protection of individuals' personal data, replacing the Data Protection Act 1998 ("**DPA**"). Many of the core data protection principles remain the same as under the DPA, but there are significant enhancements that need to be addressed in order to comply with the GDPR.

Policy statement:

Bexley Moorings Project (BMP) will make it generally known to service users, staff and volunteers, students, Board members and any other people data may relate to (data subjects), what personal data is stored, why and how it is processed in the ordinary course of our business. Most personal data held by BMP is processed in the performance of its contacts with either service users or staff and requirements of contracts with third parties and regulatory bodies such as the Charity Commission and Companies House.

BMP is committed to the protection of the rights and freedoms of individuals in accordance with the provisions of the GDPR. We will comply fully with the requirements of the GDPR, and any subsequent legislatives updates, and will follow procedures which aim to ensure that all persons who have access to any personal data held by or on behalf of BMP are fully aware and abide by their duties and responsibilities of the legislation.

We will ensure that all personal information is processed properly, however it is collected, retained, used or otherwise processed: on paper, electronically, or recorded by any other means. Accurate, proportionate and up to date records are kept ensuring a good framework of support and supervision for volunteers, employees and to comply with employment, charity and other legal requirements.

Definitions

For the purposes of this policy, the following definitions shall apply:

"personal data/ information"
Any information relating to an identified or identifiable natural person (**"data subject"**); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as names, addresses, telephone numbers, job titles, date of birth, salary, ID numbers, location data, online identifiers, genetic data or biometric data.

The GDPR lists **"special categories of personal data"** which includes:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;
- genetic and biometric data; and
- data concerning health, a natural person's sex life or sexual orientation

GDPR Data Protection Principles
BMP will comply with the data protection principles of the GDPR to ensure all personal data is:

- processed lawfully, fairly and in a transparent manner;
- obtained for specified, explicit and legitimate purposes only;
- only processed in a way that is compatible with the purpose(s) for which it was collected;
- adequate, relevant and limited to what is necessary for the relevant purpose(s);
- accurate and up to date;
- kept for no longer than is necessary for the purpose(s) for which the data is processed;
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorized processing, access, loss, destruction or damage.

<u>The Board of Trustees</u>

BMP's compliance with the GDPR is the overall responsibility of Trustees Board (**"the Board"**).

The Board will review and rectify a GDPR compliance statement for use with third parties, regulatory bodies and families.

(a) <u>Data Protection Lead</u>

The Board will appoint a named Data Protection Lead, who shall:

- inform and advise BMP and its employees who carry out processing of their obligations pursuant to the GDPR.
- monitor compliance with the GDPR, including the assignment of responsibilities, awareness-raising and training of employees, trustees and volunteers involved in processing operations, and the related audits.
- oversee, and provide advice where requested on the annual process of reviewing data protection impact assessments ("**DPIA**") – more detail on DPIAs is set out below.
- oversee progress with the action log and risk register.
- co-operate with and act as the key contact point for the Information Commissioner's Office ("**ICO**") on issues relating to BMP's data processing, including personal data breaches and any necessary DPIA consultations.

Employees, Trustees and Volunteers

It is the responsibility of all employees, trustees and volunteers to comply with this policy and to conduct themselves with integrity and in a way which considers the rights and freedoms of children, young people, parents and families at all times. Every individual has a critical role to play in the correct processing and control of personal data and sensitive categories of data. They are required to:

- familiarise themselves with the provisions of the GDPR and ensure they understand their individual responsibilities (including but not limited to keeping personal data and other confidential information secure) and to seek guidance from their line manager if they are unclear as to the application of the GDPR to their role.
- read and comply with this policy and attend all training sessions in relation to data protection as relevant to their role.
- ensure any information they provide in connection with their employment / engagement is accurate and up to date and inform BMP of any changes to information that they have provided, e.g. changes of address or changes to the bank or building society account to which the individual is paid (if applicable).
- reporting security risks and personal data breaches in accordance with this policy.

Review Process

BMP actively manages the personal data which is collected, retained or otherwise processed through an annual review cycle. The annual review cycle will include an identified register of information flows, associated DPIAs and a resulting action log. An information risk register will be maintained and reviewed by the Board. All this documentation should be reviewed at least annually by the Data Protection Lead.

Data Protection Impact Assessments (DPIA)

BMP will identify all the areas where we process personalised information (processing activities). A register of information flows should be held and DPIAs must be carried out annually for all processing activities.

A DPIA must also be carried out when any new technologies are introduced to the scheme and whenever a new processing activity is likely to result in a high risk to the rights and freedoms of individuals.

A DPIA should contain:

- A description of the processing operations and the purposes, including where applicable, the legitimate interests pursued by the GDPR lead.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that BMP comply.

Note: A DPIA can address more than one project.

Registration

Bexley Moorings Project schemes shall ensure they have obtained all authorisations and registrations and provided all notifications necessary under the data protection legislation in order to lawfully carry out its data processing activities.

Subject Access Requests

Individuals have the right to access their personal data and supplementary information, amongst other things, to allow such individuals to be aware of and verify the lawfulness of the processing. (see Subject Access Request policy)

Erasure

Individuals have the right to request that any of their personal data held by BMP be erased ('right to be forgotten'). The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

BMP may refuse the request in limited circumstances, including for public health purposes in the public interest and the exercise or defense of legal claims.

To the extent that BMP has disclosed any personal data to any third parties, it shall inform such parties about the request for erasure, unless it is impossible or involves disproportionate effort to do so.

Personal Data Breach

All employees, trustees and volunteers must report and co-operate in the resolution of all personal data breaches in accordance with this Section 7.8 and the flowchart at Appendix 1 of the personal data breach policy. This shall also include where a data protection control has failed but has not resulted in a breach (a 'near miss').

BMP (when acting in its capacity as data controller) is obliged under the GDPR to record all personal data breaches and notify the ICO of any breaches that fall within the criteria and time limits defined by the ICO.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, we must directly notify all those individuals affected by the breach without undue delay. This should not been done by any employees, trustee or volunteer without first notifying the Data Protection Lead (or in their absence the Chair).

External processors

BMP will ensure that data processed by external data processors (for example service providers, cloud services and website hosts) are compliant with this policy and all relevant data protection legislation. Their GDPR compliance statement should be seen and a written contract / undertaking entered into containing at least the minimum information required by the data protection legislation and all associated guidance notes.

This policy needs to be read in conjunction with:

Personal Data Breach Policy
Subject Access Policy

Policy agreed:

Date: 28/4/26

Review Date: 28/4/27.