BROMLEY Y DATA PROTECTION POLICY

This policy covers all the activities and processes of Bromley Y that use personal information in any format. It relates to all Bromley Y staff and others acting for or on behalf of Bromley Y when accessing personal information. This policy applies in conjunction with specific procedures and guidelines.

1. BACKGROUND

1.1 Bromley Y is a data controller under the General Data Protection Regulation. The organisation holds and processes personal data across offices and in a variety of formats (paper and electronic records). Personal information is essential to the operations of Bromley Y and should be managed with care, in confidence and in compliance with the requirements of the General Data Protection Regulation.

1.2 General Data Protection Regulation definitions are as follows:

- **Personal data:** information relating to an identifiable person who can be directly or indirectly identified (in particular, by reference to an identifier).
- **A controller:** determines the purposes and means of processing personal data.
- **A processor:** is responsible for processing personal data on behalf of a controller.
- **Processing:** any operation performed on personal data, including collection, storage, analysis, transfer, destruction.
- **'Special categories of personal data'** (GDPR Article 9) covers sensitive personal data which requires an increased level of protection. For example, information about a person's: race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation.

2. REGISTRATION

2.1 In compliance with data protection legislation, Bromley Y are registered with the Information Commissioner's Office (ICO). The organisation will inform the ICO of any changes to processing of personal information and will keep registration details up to date.

3. DATA PROTECTION PRINCIPLES AND DATA SUBJECT RIGHTS

3.1 Bromley Y will manage the processing of personal information in compliance with the data protection principles set out in Article 5 of the General Data Protection Regulation. Personal data should be:

- "processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;

- 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; and
- 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."

3.2 Data Subjects have the following rights under the GDPR:

- The right to be informed: an obligation for organisations to provide 'fair processing information' (this emphasises the need for transparency is the use of personal data).
- The right of access: the individual's right to access their personal data and supplementary information.
- The right to rectification: individuals have the right to have personal data rectified if it is inaccurate or incomplete.
- The right to erasure: also known as 'the right to be forgotten' to allow an individual to request the removal of personal data where there is no compelling reason for its continued processing.
- The right to restrict processing: individuals have a right to suppress processing of personal data under certain circumstances, unless the organisation has overriding legitimate grounds for processing.
- The right to data portability: allows individuals to move, copy or transfer personal data from one IT environment to another in a safe and secure way, without affecting usability.
- The right to object: individuals have the right to object to processing of their data under certain circumstances, unless the organisation has overriding legitimate grounds for processing.
- Rights in relation to automated decision making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual).

4. THE PRINCIPLES IN PRACTICE

4.1 Bromley Y will comply with the data protection principles and will undertake the following steps:

- Confidentiality: information should be kept securely where necessary and protected from non-authorised disclosure.
- All information records are to be managed to ensure confidentiality, reliability, authenticity, integrity and usability.
- When collecting personal information, Bromley Y will clearly state what the information will be used for, the legal basis for processing, who will have access to information and for what purpose. Bromley Y's GDPR exceptions for processing special categories of data include:
    - Fulfilling the obligations of controller or of the data subject.
    - Protecting the vital interests of the data subject.
    - Processing carried out by a foundation or not-for-profit organisation.

- Reasons of public interest in the area of public health.
- Collection and use of personal information will be kept to a minimum for specific stated purposes.
- Bromley Y will apply processes to personal information collection, use and maintenance to increase quality and reduces risks of inaccuracy and unnecessary duplication.

4.2 Retention and disposal procedures: records should not be retained for longer than they are needed and should be disposed of in line with business need and relevant legislation/best practice. A Records Retention Schedule will be maintained to determine required personal information retention and timely destruction (physical and electronic copies of information). This will include requirements for destruction such as shredding of hard copies and deletion of files from hardware and from cloud-based backups.

4.3 Rights of data subjects under the GDPR will be respected:

- The right of subject access (the right of individuals to have a copy of information Bromley Y holds on them) will be supported by a Subject Access Request Procedure/Process.
- Individuals right to rectify their data will be supported by a Data Rectification Procedure.
- A Client Data Quality Process to ensure personal data is of sufficient quality to make decisions about individuals.
- A Data Breach Reporting Procedure detailing breach/incident reporting and guidelines for escalating the situation to the Information Commissioner's Office.
- Individuals rights in general will be outlined within the Client Privacy Policy.
- Data Controller/Data Processor Contracts are implemented for suppliers to ensure an adequate level of protection for any personal data processed on Bromley Y's behalf.
- Bromley Y will does not intend to transfer data outside the European Economic Area – cloud-based provider Data Centres are based within the United Kingdom.
- Children's data: consent (such as for video recording) - if the child is under 16, informed consent should be gained from the parent or carer where relevant/possible.

4.4 Bromley Y will consider personal data protection for all new projects/initiatives to ensure a privacy by design approach. The requirement for a data protection impact risk assessment will be considered for all new initiatives and records will be kept of the outcomes of these assessments.

4.5 A Data Protection and Information Security Risk Assessment will be conducted/updated annually and reported to Trustees.

4.6 The Protection and Security of Personal Information: Bromley Y will maintain an Information Security Policy and framework of technical measures to ensure appropriate levels of security are in place to adequately protect personal information it controls and processes. Security breaches will be assessed and subject to appropriate actions and breach reporting (for further details, please see Bromley Y's Information Security Policy).

4.7 Awareness and Training: Bromley Y will provide guidance, support and training on the management of personal information and relevant legislation to all staff. Guidance on data protection will also be provided to all those acting on behalf of Bromley Y.

5. REVIEWS AND CONTINUOUS IMPROVEMENT

5.1 The processes for managing personal information will be intermittently audited, reviewed and any recommendations implemented as part of a continuous process of improvement.

6. PERSONAL INFORMATION MANAGEMENT POLICY ROLES AND RESPONSIBILITIES

6.1 Bromley Y's Data Protection Policy is agreed by the Board of Trustees. The Director and the identified Data Protection Officer (currently the Data Manager) are responsible for maintaining this data protection policy, the information security policy and associated procedures/processes. This includes but is not limited to:

- Maintaining the Records Retention Schedule.
- Managing formal subject access requests.
- Managing procedures/processes relating to data protection.
- Providing guidance, support and training on personal data management and data protection legislation.
- Liaison with the Information Commissioner's Office on data protection issues.

All Senior Managers are responsible for ensuring awareness and compliance with this policy. Staff, contractors and suppliers who handle personal information for or on behalf of Bromley Y are responsible for its security and compliance to the requirements of the GDPR.

Any personal data security breach, personal data damage or personal data loss should be reported to the Director and Data Protection Officer. Mishandling of personal data could lead to a disciplinary investigation and additionally could be a breach of the law. Staff are advised to seek guidance from the Director and Data Manager if any concerns arise.

This policy should be read in conjunction with the following:

- *Information Security Policy*
- *Confidentiality Policy*
- *Equipment and Data Disposal Policy*
- *Acceptable Information Technology Use Policy*

10. MONITORING AND REVIEW

The Board of Trustees, will regularly review the operation of this policy.

This policy has been approved and authorised by the Trustees of Bromley Y

Signature: .....

Date: .....