DATA MANAGEMANT POLICY

Principles

This Policy is intended to ensure the effective, efficient and compliant management of information and data held and used by **Rainbow Stop Playgroup**. The policy statement will support continuous improvement in the organisation's core activities, provide evidence of corporate governance, and facilitate compliance with statutory requirements.

Rainbow Stop Playgroup are fully committed to compliance with the requirements of the Data Protection Act 1998 and aim to ensure that only relevant information is collected, processed and stored appropriately. In line with the General Data Protection Regulations (GDPR), which applies from 25 May 2018, **Rainbow Stop Playgroup** have developed clear procedures to protect personal data, and have adopted appropriate technical and organisational measures to remain compliant.

The Data Management Policy applies to all staff, committee members, volunteers and other individuals or partner organisations undertaking collaborative activities. The policy covers all information and data held by the organisation whether held electronically or in hard copy.

Policy

In order to operate efficiently, **Rainbow Stop Playgroup** must collect and use appropriate and relevant information. In addition, it may be required to collect and use information in order to comply with funders and partner organisation requirements.

The Data Management Policy is designed to ensure that **Rainbow Stop Playgroup** manages data and information in ways which support business efficiency, legal requirements and the rights of individuals. As part of our commitment to the Data Protection Act 1998 and the General Data Protection Regulations (GDPR), **Rainbow Stop laygroup** will adhere to the legislation and the following Data Management Principles.

Data Management Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations. These may evolve when the new GDPR legislation comes into force.
Article 5 of the GDPR requires that personal data shall be:

"a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) 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;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) 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;

e) 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

f) 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."

There is a new addition for GDPR, which is known as the "accountability principle" which is reflected in Article 5(2) below:

Article 5(2) requires that: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

Procedures

This policy will be implemented via the introduction of a Data Management Procedure. All staff are expected to comply with the procedures which support this policy.

Responsibility

All Staff

All staff, committee members, volunteers other individuals and partner organisations are responsible for following this policy and adhering to data and information management procedures. All staff are responsible for ensuring accurate information and data management procedures are followed in their work. This includes the collation of data, the processing of information and the systems and practices used. Staff have responsibility to ensure that their activities comply with the Data Management Principles.

Staff should not disclose information or data to persons who are not authorised to receive it or outside the organisation's procedures, or use information or data held on others for their own purposes.

All staff are responsible for documenting their work and keeping records in line with **Rainbow Stop Playgroup** policies and procedures, disclosing information only to those who need to have access to it in the course of their duties.

Staff will not retain information for longer than is required for a particular purpose.
Committee Members and Managers

Committee Members and Managers are responsible for ensuring the implementation of the Data Management Policy and Procedures and that all staff are aware of their responsibilities under this Policy, reporting and dealing with any suspected malpractice.

Committee Members have responsibility to ensure that only relevant information is collected, processed and stored appropriately in accordance with current and future legislation.
Committee Members are responsible for providing adequate and appropriate electronic and physical storage facilities to support record keeping across the organisation.

Training

Managers will identify and provide staff with access to training, support and guidance and advice on data management and any further training necessary to ensure compliance with the General Data Protection Regulation (GDPR).

Protocol for Reporting Breaches

A data security breach can happen for several reasons including inadequate password protection; human error, e.g. sending data to the wrong person; leaving a computer unattended; and hacking. In the event of a data security breach, the matter must be logged and reported to the committee. The Committee must take appropriate action in line with the GDPR and their own Policies and Procedures. The nature and cause of the breach must be identified to ensure the breach does not re-occur.

DATA AND RECORD MANAGEMENT PROCEDURE

PURPOSE

The purpose of this procedure is to detail data and records, whether physical or electronic, held by **Rainbow Stop Playgroup**, the length of time that these should be retained by the Setting, and provide guidance on archiving and destroying data and records that are no longer required to be kept. This procedure will be superseded by other contractual requirements that may be required to maintain compliance. This procedure promotes consistency by ensuring that the setting keeps the same data and records for the same period of time.

SCOPE

This procedure applies to all **Rainbow Stop Playgroup** management committee members, trustees, directors, staff, volunteers, placement students (herein referred to as staff).

DATA AND RECORD RETENTION

Data and records must be kept securely, retained for the appropriate time and destroyed when it is appropriate to do so. The retention period of data and records may be adjusted in line with contractual obligations to meet the requirements of funding bodies and legislation.

A matrix of data and records sets out the type, location of storage, holder, retention and archive periods and disposal methods including data and records held in relation to staff.

All data and records, held by each staff member, should be reviewed annually. This will ensure that any duplicate or non-relevant data and records can be archived or destroyed. Management Committees members and staff will ensure that once files are no longer required to be kept in current systems that they should be archived or destroyed as appropriate.

Physical Data and Records

During the annual review process data and records should be reviewed, maintained or disposed of appropriately.

Electronic Data and Records

Electronic data and records should be, where possible, stored in shared folders to avoid unnecessary duplication. Confidential data and records should be secured. Pen drives and external devices should not be used as a storage medium, unless the data or device is password protected or encrypted. Use of these devices must be authorised by the relevant Manager. Confidentiality and security of electronic data and records is crucial. Staff are required to ensure that confidential data and records are not shared with persons who are not authorised to receive it.

DATA AND RECORD ARCHIVING

Data and records that are no longer required to be retained in current storage should be archived annually.

Physical and Electronic Data and Records

Following the annual review of physical and electronic data and records, archived files should be clearly labelled with the title and the date of the life span of the information held within it, or if electronic this should be given an appropriate file name. Physical data and records contained within archive files should be stored chronologically and papers sub-divided for easy retrieval. Documents should be kept clean and tidy and be fixed into the file and not loose. Electronic data should be catalogued into an appropriate folder structure for easy retrieval.

Archive boxes should contain files which relate to each other to ensure easy retrieval of information. Once placed into the relevant archive box, the name and date of the file and the date when the file should be removed from archive storage and destroyed, should be clearly and legibly displayed on the front of the box. A record of each archived box and the names of the files in the box (title, date of the life of the file and date the file should be removed from archive) must be kept by relevant staff. If data is archived locally, the archived documents should be stored securely in a safe place when not in use.

Archive boxes should be stored in a secure place within the relevant office, or contracted out to a specialist archiving company. Section 6 outlines the process that should be used for archiving data and records.

In terms of electronic data archiving please adhere to the ICT Policy in regard to storage, transfer and archiving of data. The ICT Policy should be adhered to at all times to ensure data security and access, whilst maintaining accuracy and minimal duplication.

DATA AND RECORD REMOVAL

Physical and Electronic Data and Records

The Archive Log should be reviewed annually by the Management Committee members and staff. This will ensure that all data and records that have reached the maximum retention period can be

destroyed. Management Committee members and staff should refer to the Records Matrix for information on the disposal method of data.

ARCHIVING PROCEDURE

Records that require archiving must be boxed, labelled and recorded using the following process:

- Records should be packed in alphabetical or chronological order whichever is appropriate.
- Do not over pack the boxes.
- Complete Archive Label and attach to the box. Complete Archive Log

End of Archiving Period and Disposal of Data

- The Archive Log, should be reviewed annually by the Management Committee members and staff. This will ensure that all data and records that have reached the maximum retention period can be destroyed.
- Management Committee members and staff should refer to the Records Matrix.

Signed:

Position:

Date: